THE JUDICIAL RESPONSE TO MASS POLICE SURVEILLANCE

Stephen Rushin†

TABLE OF CONTENTS

I. Introduction 282
II. The Digitally Efficient Investigative State 284
A. Examples of Emerging Technologies in the Digitally Efficient Investigative State 285
1. Automatic License Plate Recognition 285
2. Surveillance Cameras and Facial Recognition Software 287
3. Law Enforcement Use of Third-Party Databases 289
B. The Declining Cost of Data Storage and Mass Recordation 291
C. Data Fusion and the Move Towards a Centralized Investigative State 292
D. The Implications of the Digitally Efficient Investigative State 294
1. Potential Benefits 294
2. Potential Harms 299
III. The Fourth Amendment and Surveillance Technologies 303
A. Defining a Search 303
B. The Distinction Between Efficiency and Intrusiveness 305
IV. Applying the Existing Fourth Amendment Doctrine to the Digitally Efficient Investigative State 309
A. Warrantless Use of ALPR is Likely Constitutional 309
B. Warrantless Use of Video Surveillance with Facial Recognition is Likely Constitutional 313
C. Warrantless Use of Third-Party Databases is Likely Constitutional 315
D. Jones as a Test Case for the Constitutionality of the Digitally Investigative State 316
V. The Judicial Response to the Digitally Efficient Investigative State 318
A. The Judicial Response 318
B. The Courts Are Better Positioned Than the Legislature to Regulate Police Technologies 322
C. Re-conceptualizing the Current Privacy Doctrine in Light of the Digitally Efficient Investigative State 326
VI. Conclusion 328

† PhD student at the University of California, Berkeley, Jurisprudence and Social Policy Program; J.D., University of California, Berkeley Law School. Special thanks to Professors Kathryn Abrams and Malcolm Feeley for their thoughtful edits and support throughout the development of this Article.

Abstract

The increasingly widespread use of police technologies like surveillance cameras, facial recognition software, and automatic license plate recognition (ALPR) systems threaten to fundamentally reshape our expectations to privacy in public spaces. These technologies are capable of recording copious amounts of personal data in an unprecedentedly efficient manner; I refer to the proliferation of these new technologies as the development of the digitally efficient investigative state. The legislative branch has not acted to address the tangible harms posed by this new technological order. I argue that the courts ought to respond to this burgeoning threat by treading a new doctrinal path to limit the indiscriminate collection of personal data. The courts are institutionally competent to craft an appropriate response and properly positioned to address the unique majoritarian concerns implicated by widespread police surveillance. I also contend that the development of the digitally efficient investigative state should serve as a medium for the courts to more systematically reassess our Fourth Amendment doctrine, in recognition of the transformative and pervasive effects of emerging technologies on individual privacy.

I. INTRODUCTION

Law enforcement technology has become ubiquitous in the urban landscape. Closed circuit surveillance cameras indiscriminately record individuals' physical movements.[1] Facial recognition software compares images of passing pedestrians with extensive databases of suspected criminals.[2] Red light cameras capture photographs of traffic violations. The National Security Agency (NSA) logs phone calls made by millions of citizens across the country in hopes of identifying suspected terrorist activity.[3] And automatic license plate recognition (ALPR) systems, already in use in various jurisdictions across the country, digitally read and record the license plates of passing automobiles into expansive databases.[4] Indeed, we live today in an increasingly digitally efficient investigative state—a state where law enforcement can both observe and record information about our whereabouts in an unprecedentedly efficient manner. The retention of surveillance data raises many serious constitutional concerns. But Fourth Amendment doctrine on search and seizures reflects outdated assumptions about the once-limited capabilities of public surveillance technologies and is, therefore, ill-equipped to deal with the challenges posed by the digitally efficient investigative state.

The existing Fourth Amendment doctrine on surveillance technologies

1. Spencer S. Hsu, *D.C. Forms Network of Surveillance: Police Video Links Raise Rights Issues*, WASH. POST, Feb. 17, 2002, at C1.

2. John J. Brogan, *Facing the Music: The Dubious Constitutionality of Facial Recognition Technology*, 25 HASTINGS COMM. & ENT. L.J. 65, 81 (2002–2003).

3. Laurie Kellman, *NSA Building Giant Database of Americans' Phone Calls; Bush Says Privacy Protected*, SEATTLE TIMES, May 11, 2006, http://community.seattletimes.nwsource.com/archive/?date=20060511&slug =webphone records11.

4. Mary Beth Sheridan, *License Plate Readers to be Used in D.C. Area*, WASH. POST, Aug. 17, 2008, at C1.

focuses primarily on three issues: (1) whether a person had a subjective expectation of privacy; (2) the socially objective reasonableness of that expectation of privacy; and (3) the relative intrusiveness of the supposed privacy violation.[5] The Supreme Court has also drawn a distinction between presumptively constitutional technologies that merely improve the efficiency of legitimate law enforcement, like digital tracking devices, and unconstitutional technologies that give law enforcement an intrusive extrasensory ability, like heat sensors.[6] Under this framework, the warrantless use of most surveillance technologies and the collection of personal data fits comfortably within constitutional doctrine—after all, a person does not have an objectively reasonable expectation to privacy when driving her car or walking on a public sidewalk. The recording of a person's movements in public is not especially intrusive and certainly does not provide police with any intrusive, extrasensory abilities beyond mere observation. A recent Seventh Circuit case engaged in just this type of analysis when it found that the warrantless use of global position system (GPS) surveillance by law enforcement did not violate the Fourth Amendment.[7] There, Judge Posner and the Seventh Circuit concluded that GPS monitoring of a single suspect without a warrant does not amount to "wholesale surveillance."[8] But Posner quickly pointed out, "Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive . . . . Should government someday decide to institute a program of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search."[9]

That time has come. The digitally efficient investigative state comes dangerously close to "wholesale surveillance." The unregulated use of these emerging technologies may incentivize police fishing expeditions, facilitate racial profiling, and corrode any notion of public anonymity. And the legislative branch has not acted to address the tangible harms posed by this new technological order. In wake of the legislative inactivity, I argue that it is finally time for the courts to break from the previous doctrinal trend and act decisively to regulate the efficiency of police surveillance technology. While a judicial response may help ameliorate some of the pressing concerns raised by the digitally efficient investigative state, it should only be the beginning of a broader re-conceptualization of our Fourth Amendment doctrine. I argue, in particular, that we ought to reassess our presumption that individuals have no reasonable expectation to privacy in their public actions. In total, I hope to make two contributions with this Article, one descriptive and one normative. Descriptively, I build a comprehensive account of the digitally efficient investigative state, and normatively I contend that the courts must establish a new doctrinal path to regulate this technological order.

I have divided this Article into four parts. In Part I, I examine the use of

5. Renée McDonald Hutchins, *Tied Up in* Knotts? *GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 427–30 (2007–2008) (citing Katz v. United States, 389 U.S. 347, 352 (1967)).

6. *Id.* at 433–39.

7. United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007).

8. *Id.* at 997–99.

9. *Id*. at 998.

ALPR, surveillance cameras with facial recognition, and third-party databases as paradigmatic examples of intrusive, emerging technologies utilized by law enforcement in the digitally efficient investigative state. In Part II, I outline the current Fourth Amendment doctrine on unreasonable search and seizures. Part III considers the constitutionality of the digitally efficient investigative state under Fourth Amendment doctrine. Finally, Part IV argues for a new doctrinal approach to regulate the digitally efficient investigative state and a broader re-conceptualization of our understanding of the Fourth Amendment.

II. THE DIGITALLY EFFICIENT INVESTIGATIVE STATE

Scholars have long suggested that the use of advanced surveillance technology may dramatically transform social expectations of privacy. Jack Balkin has argued that the introduction and integration of mass surveillance technologies into urban centers has created a National Surveillance State.[10] According to Balkin, the National Surveillance State focuses principally on preventing criminality ex ante, as opposed to prosecuting crime ex post.[11] The coordination of the state with private companies has allowed the National Surveillance State to circumvent constitutional limitations.[12] Other scholars have similarly warned about the threats of mass surveillance and data collection by the state.[13] But there is a surprising dearth of scholarship on the expanding use of ALPR and policing surveillance cameras with facial recognition software. In this Part, I offer a reasonably comprehensive, descriptive account of the capabilities and threats posed by the digitally efficient investigative state.

I begin this Part by first examining the use and capabilities of several common surveillance technologies including ALPR, surveillance cameras with facial recognition software, and third-party databases. In particular, I focus on how each of these technologies can be used for two separate and constitutionally distinguishable purposes: observational comparison and indiscriminate data collection. Second, this Part will discuss the increased feasibility of high density, low-cost data retention, and the move towards the centralization of surveillance data to facilitate data sharing across police departments. Finally, I draw on psychological and behavioral research to assess the constitutionally relevant implications of the digitally efficient investigative state. In total, this Part will demonstrate the impressive, efficient, and ultimately intrusive capabilities of the unregulated use of surveillance technologies.

---

10. Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 3–4 (2008–2009).

11. Orin S. Kerr, *The National Surveillance State: A Response to Balkin*, 93 MINN. L. REV. 2179, 2179 (2009) (citing Balkin, *supra* note 10). In this Article I focus primarily on the use of efficiency-enhancing technology by public law enforcement. I spend some time addressing the use of private data by public actors, but this public-private intersection raises countless other constitutional and privacy issues that are not addressed within the narrow scope of this Article.

12. *Id*.

13. *E.g.*, Daniel J. Solove, *Digital Dossier and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1095, 1102 (2002) (referencing that government information-collection interferes with personal freedom of association and implicates the right to speak anonymously).

A. Examples of Emerging Technologies in the Digitally Efficient Investigative State

1. Automatic License Plate Recognition

The use of ALPR raises concerns of both surveillance and extensive data collection. ALPR is a relatively new technology that was first used in Britain over the last two decades to protect against Irish Republican Army attacks.[14] Since then, ALPR has become a common law enforcement tool used by police departments across the world, including many jurisdictions in the United States.[15] ALPR uses digital cameras mounted on a law enforcement vehicle or at stationary locations to snap images of passing license plates.[16] When a vehicle approaches, the ALPR device takes a series of photographs and stores them in a digital file.[17] The most advanced license plate readers photograph up to 1,800 plates per minute at a speed of up to 140 miles per hour.[18] These digital photographs are transmitted to a computer system inside of the vehicle and optical character recognition software converts the plate numbers in the photographs into text.[19] Once converted, the ALPR system compares the plate numbers to available databases, often called hotlists, including lists of stolen automobiles, active arrest warrants, and AMBER alerts.[20] I describe this ability to read passing license plates, compare them to known criminal databases, and flag suspected offenders as the *observational comparison* feature of ALPR. When used for observational comparison, ALPR only retains data on license plates that match known or suspected criminal hotlists. Hence, the observational comparison utility is an incredibly efficient law enforcement tool that is reasonably tailored to only flag the suspicious.

But many departments across the country are using ALPR not just for

---

14. Sheridan, *supra* note 4, at C1.

15. *See, e.g.*, *High Tech License Tag Reader Leads to Arrests*, NEWARK POST, Oct. 7, 2010, http://infoweb.newsbank.com/iw-search/we/InfoWeb?p_product=AWNB&p_theme=aggregated5 &p_action=doc&p_docid=132BD1431A788128&p_docnum=1&p_queryname=1 (discussing ALPR use in Delaware); Michelle Webster, *New Police Weapon Nabs 144 Drivers*, ILLAWARRA MERCURY (Nov. 1, 2010, 12:00 AM), http://www.illawarramercury.com.au/news/local/news/general/new-police-weapon-nabs-144-drivers/1984027.aspx?storypage=0 (discussing ALPR use in Australia). It is worth noting that only one study has explored the extent to which ALPR technologies are used by local law enforcement. This study, completed by the International Association of Chiefs of Police in 2010, found that the majority of departments do not currently use the technology, but nonetheless have a positive view of the technology. Roughly 40% of the 500 departments surveyed indicated that they currently utilize some form of ALPR, but many were unwilling to complete a survey on their usage, citing confidentiality concerns. *See* National Law Enforcement and Corrections Technology Center, *The Results Are In: Automatic License Plate Technology Leads to Success*, TECH BEAT, 1 (2010), http://www.justnet.org/TechBeat%20Files/Automatic%20License%20Plate%20Reader.pdf.

16. Ken Belson, *The Wired Repo Man: He's Not 'As Seen on TV'*, N.Y. TIMES, Feb. 28, 2010, at AU 1; Int'l Ass'n of Chiefs of Police Nat'l Law Enforcement Policy Ctr., *License Plate Readers*, Aug. 2010, at 1–2 , http://www.mass.gov/Eeops/docs/programs/ghsb/alpr2011/alpr_license_plate_white_paper.pdf [hereinafter IACP Policy Center].

17. *An Introduction to ANPR*, CCTV INFORMATION: FROM THE CCTV ADVISORY SERVICE, http://www.cctv-information.co.uk/i/An_Introduction_to_ANPR (last visited Sept. 7, 2010).

18. Press Release, ELSAG, ELSAG North America Introduces New Tactical Operation Center (TOC) Software and All-In-One Fixed Plate Hunter (AIO) at 2010 IACP Show (Oct. 27, 2010), *available at* http://www.elsag.com/detail.asp?i=309.

19. Belson, *supra* note 16, at AU 1.

20. *See* Sheridan, *supra* note 4, at C5; IACP Policy Center, *supra* note 16, at 3.

observational comparison, but also for *indiscriminate data collection*.[21] When used in this manner, ALPR systems not only flag passing cars that match a criminal database, but they also record the exact time and location of *all passing cars* into a searchable database, whether or not there is any evidence of wrongdoing.[22] This data can be kept on file indefinitely.[23] In communities with extensive, integrated networks of ALPR cameras, this could potentially amount to mass surveillance of an entire community. As a Los Angeles Police Department Chief of Detectives explained, "The real value [of ALPR] comes from the long-term investigative uses of being able to track [all] vehicles—where they've been and what they've been doing."[24] Theoretically, by mounting ALPR at every intersection and on every police car in a city, it is conceivable that the police could begin to compile thousands of discrete data points, each data point indicating the time and location of an automobile.

Law enforcement can often easily determine the likely driver of a given car by cross-referencing a license plate number with state motor vehicle records. In this way, the license plate characters collected by ALPR systems can be classified as personally identifiable information.[25] With enough ALPR systems installed in a community, the police could ultimately create an accurate and pervasive record of a person's movements over months, or even years. There are, of course, potential investigative benefits to such indiscriminate data collection. Imagine if, upon receiving a report of a child abduction, police officers could immediately ascertain the name and address of all drivers in the vicinity at the time of the abduction. Privacy advocates have, though, expressed concern that ALPR can amount to mass surveillance and lead to extensive law enforcement abuse.[26] In Birmingham, United Kingdom, for instance, law enforcement used ALPR to closely monitor the daily movements of a largely Muslim community, inciting allegations of racial profiling.[27] At least two states, New Hampshire and Maine, have enacted legislation to limit the collection of indiscriminate data via ALPR.[28] Most states and localities, though, have done little to regulate this emerging

---

21. Brian Alseth, *Automated License Plate Recognition: The Newest Threat to Your Privacy When you Travel*, ACLU OF WASH. BLOG (May 26, 2010, 9:31 AM), http://www.aclu-wa.org/blog/automated-license-plate-recognition-newest-threat-your-privacy-when-you-travel.

22. Hilary Hylton, *License-Plate Scanners: Fighting Crime or Invading Privacy?*, TIME, July 30, 2009, http://www.time.com/time/nation/article/0,8599,1913258,00.html.

23. *Id*.

24. Alseth, *supra* note 21.

25. INT'L ASS'N OF CHIEFS OF POLICE, PRIVACY ASSESSMENT REPORT FOR THE UTILIZATION OF LICENSE PLATE READERS 7 (Sept. 2009), *available at* http://www.theiacp.org/LinkClick.aspx?fileticket= N%2bE2wvY %2f1QU%3d&tabid=87 [hereinafter IACP PRIVACY ASSESSMENT] (defining personally identifiable information as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked to a specific individual, such as date and place of birth, mother's maiden name, etc."). The Driver's Privacy Protection Act, 18 U.S.C. §§2721-25 (1994), does not classify license plate numbers as personally identifiable information in §2725(4), but does note the privacy concerns raised by combining driver's license numbers with other personal information like a driver's name, address, telephone number, or identification number.

26. *See* Sheridan, *supra* note 4, at C5 (discussing advocates' concerns with what is done with the data after it is collected).

27. Paul Lewis, *Police Surveillance of Muslims Set Up With 'No Regard for Law,'* THE GUARDIAN, Sept. 30, 2010, http://www.guardian.co.uk/uk/2010/sep/30/police-surveillance-muslims-no-regard-law.

28. N.H. REV. STAT. §236:130 (2011); ME. REV. STAT. 29-A, § 2117-A (2009); Alseth, *supra* note 21.

technology.[29] And the federal government has taken no specific action to regulate ALPR data retention.[30]

2. *Surveillance Cameras and Facial Recognition Software*

The combination of video surveillance and facial recognition software presents another compelling example of the digitally efficient investigative state. Some may argue that video surveillance that does not compile an extensive digital record amounts to a reasonable substitute for traditional police observation.[31] But when video surveillance is coupled with facial recognition software and used for wholesale data retention, the technology transforms into an incredibly omnipresent investigative tool.

A vast majority of law enforcement agencies in the United States currently use video surveillance.[32] According to a 2001 study done by the International Association of Chiefs of Police (IACP), over 80% of American police departments have already employed video surveillance.[33] That number has, in all likelihood, increased since the survey, as half of the remaining departments indicated that they anticipated using video surveillance in the near future.[34] But the types of video surveillance used by police departments can vary greatly from one jurisdiction to another. Some jurisdictions currently use rudimentary video surveillance exclusively in a select number of high-crime public locations, while other jurisdictions have a well-developed surveillance network capable of tracking suspects with surprising accuracy.[35] In Washington, D.C., for example, law enforcement uses an advanced network of surveillance cameras linked together with hundreds of government cameras already in use by various agencies in locations throughout the city.[36] Washington, D.C., in the wake of the September 11th terrorist attacks, was the first city in the United States to not only link together an extensive network of cameras but also to create a system that digitally records all images for future reference.[37] As a result, video surveillance is no longer a mere substitute for visual observation—as the cost of storing digital information decreases, law enforcement is capable of efficiently recording a detailed history of people's movements over long periods of time.

Perhaps most disconcerting, departments across the country are now using facial recognition software in conjunction with video surveillance.[38] The

---

29. IACP PRIVACY ASSESSMENT, *supra* note 25, at 19.

30. *Id*. at 19 (noting that U.S. Department of Justice Federal Regulations on Criminal Intelligence Systems Operating Policies, 28 C.F.R. Part 23, do not apply to ALPR data since ALPR data is considered factual data, not criminal intelligence information).

31. Marc Jonathan Blitz, *Video Surveillance & the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Images & Identity*, 82 TEX. L. REV. 1349, 1354 (2004) ("The vast majority of images captured . . . are likely to receive little scrutiny.").

32. Hsu, *supra* note 1, at C4.

33. *Id*.

34. *Id*.

35. *See id*. (citing New York's use of surveillance in slashing crime in public housing, and the addition of cameras to high traffic areas of the city).

36. *Id*. at C1.

37. *Id*. at C4.

38. *See generally id*. (discussing the viability of facial-recognition software and its testing in cities and

use of facial recognition, in conjunction with other public databases like Department of Motor Vehicles (DMV) picture catalogs, permit law enforcement to identify the individuals captured by surveillance cameras. DMVs in many states already catalog the pictures taken for driver licenses and load these photographs into a searchable database.[39] Thirty-seven states currently load driver's license photographs into state databases, which are searchable using facial recognition software.[40] Facial recognition software has already been combined with video surveillance and used by law enforcement to identify potential suspects amongst large crowds.[41] During the Super Bowl in 2001, FaceTrac technology was used to digitally scan 128 points on the face of each fan entering Raymond James Stadium in Tampa, Florida.[42] This information was then compared to Federal Bureau of Investigations databases.[43] In total, the technology was able to identify nineteen suspected criminals.[44] Similar technology has been employed in major cities across the country including Boston, Tampa, Providence, Kansas City, and Washington, D.C.[45]

By themselves, video surveillance and facial recognition software do not appear particularly problematic. But when used in combination, these technologies could have Orwellian implications. Like ALPR, the capabilities of video surveillance with facial recognition can be divided between observational comparison and indiscriminate data collection. If used merely for observational comparison, the video surveillance with facial recognition would be reasonably tailored: law enforcement could compare the faces of passing pedestrians with the faces of known suspects on criminal hotlists, thereby assisting law enforcement in locating suspected criminals for questioning or arrest. In such a situation, the facial recognition software would only flag and retain information about individuals who match criminal databases. When using merely an observational comparison utility, the collection of data would be limited to individuals whose appearance so closely resembles a known criminal as to create reasonable, individualized suspicion.

It is not inconceivable that in the future, a community could employ an extensive network of surveillance cameras designed to indiscriminately accumulate data on individuals regardless of any suspicious behavior. Each of these cameras could conceivably use facial recognition software and DMV databases to identify the name of each passing individual. The digitally efficient state could then log the identity, time, and location of the person into an extensive database, which could be searched for information in future police investigations. Such technology would undoubtedly be enormously beneficial

---

airports).

39. Joey Bunch, *Smile 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.

40. *Id*.

41. Brogan, *supra* note 2, at 80.

42. *Id*.

43. *Id*.

44. *Id*. It should be noted that the use of facial recognition software here did not result in arrests. It was simply to test its future viability.

45. *Id*. at 80–81.

to law enforcement. Imagine if the police could someday identify the name and address of every possible witness to a crime. Or, imagine if police could verify alibis of suspected criminal defendants through checking a community's extensive video surveillance records. In such a digitally efficient state, law enforcement would certainly be more effective and accurate, and (assuming actors behave honestly) the community would be safer. But on a visceral level, the assemblage of extensive data on every person without any suspicion seems to elicit serious suspicion—it implies distrust and treats every individual as a potential criminal suspect at all times.

Some communities have already responded to this potential threat by crafting legislation.[46] The State of Virginia House of Delegates passed a bill that requires law enforcement to get judicial approval before installing facial scanning technology, limiting the technologies use to situations where it is likely to provide information about a felony.[47] The Virginia bill also bars law enforcement from retaining a person's image in a database unless the facial recognition software matched her to a potential crime.[48] But with some notable exceptions like Virginia, the use of facial recognition and video surveillance remains surprisingly unregulated.

3. Law Enforcement Use of Third-Party Databases

Another significant threat to privacy is the compilation of extensive personal data by private organizations. This information often moves through voluntary "information flows" to law enforcement to aid in criminal investigations.[49] That is to say, private companies often voluntarily disclose extensive collections of personal data to law enforcement including credit card expenditures, telephone records, web-surfing habits, e-mail records, and financial transactions.[50] Typically, this occurs through private company compliance with law enforcement requests.[51] This voluntary information flow hastened during the War on Terrorism.[52]

For example, after the terrorist attacks in New York City on September 11th, 2001, the Bush Administration began an extensive effort to monitor phone communications that could potentially be linked to terrorist networks.[53] In May 2006, news broke that the NSA had created a massive government database containing the phone records of millions of Americans.[54] The NSA program did not involve the listening to any phone calls without a warrant.[55]

---

46. H.B. 454, 2002 Leg., Sess. (Va. 2002).

47. *Id.*; *see also Facial Scan: Beach's Use Restricted Under Bill Approved by House*, THE VIRGINIAN-PILOT & LEDGER STAR, Feb. 13, 2002, at B4.

48. H.B. 454, 2002 Leg. Sess. (Va. 2002).

49. Solove, *supra* note 13, at 1095 (citing Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315 (2000)). *See also* Joel Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 550 (1995).

50. Solove, *supra* note 13, at 1095–1101.

51. *Id*.

52. *Id*.

53. *See, e.g.*, Susan Page, *Furor Erupts Over NSA's Secret Phone Call Database: Disclosure of Program Reignites the Debate on Liberty vs. Security*, USA TODAY, May 12, 2006, at 1A.

54. Kellman, *supra* note 3.

55. *Id*.

Instead, the NSA merely collected phone records voluntary turned over by Verizon, AT&T, and other major phone companies.[56] Using this information, the NSA examined the records using advanced software to detect any suspicious patterns that may have suggested terrorist activity.[57] For example, the NSA would flag phone calls from the Middle East to the United States "if the person receiving the call subsequently made a domestic call."[58] The NSA would then attempt to connect the flagged phone numbers to a list of suspected terrorist numbers.[59] And the NSA intends to keep this data indefinitely.[60] This NSA program elicited major political backlash, with many politicians and privacy advocates claiming that surveillance of phone call patterns gives the government an intimate look into an individual's private life.[61] Yet many defended the NSA program, arguing that it provided the NSA with a vital tool to fight terrorism that minimally invades privacy.[62] Proponents compared this technology to a digital phone book, assuring Americans that the NSA had no intention to spy on the activities of average Americans.[63] But others have challenged the NSA database as a blatant violation of federal law.[64]

Ultimately, the NSA program is but one of many examples of expansive database information flowing from private companies to law enforcement to assist in ongoing investigations. This presents a unique legal challenge; after all, the state is in no way compiling this information—private parties like phone companies compile the information for billing purposes and then voluntarily hand it over to law enforcement. Company privacy disclosures often leave leeway for disclosure of personal information to assist in government investigations.[65] Individuals knowingly and voluntarily turn over information to private organizations by doing business with that company. This can be understandably contrasted with information collected by the state through public surveillance. Nonetheless, the warrantless use of this privately compiled data has the same functional effect—law enforcement gains a potentially intimate and pervasive look into the personal life of countless innocent individuals.

Overall, these emerging technologies—ALPR, surveillance cameras, facial recognition software, and third-party databases—dramatically improve investigate efficiency. And these technologies are merely the tip of the investigative iceberg. Red light cameras, warrantless GPS surveillance, and other investigative tools are also widely used across the country. These

---

56. *Id*.

57. *Id*.

58. Andrew P. MacArthur, Note, *The NSA Phone Call Database: The Problematic Acquisition and Mining of Call Records in the United States, Canada, the United Kingdom, and Australia*, 17 DUKE J. COMP. & INT'L L. 441, 444 (2007).

59. *Id*.

60. *Id*.

61. *See, e.g.*, Tim Reid, *Bush May Have Crossed the Line by Tracking Every US Phone Call*, TIMES (U.K.), May 12, 2006, at 53.

62. Interview by Noah Adams with John Cornyn, Sen., Texas (May 12, 2006) (transcript available at http://www.npr.org/templates/story/story.php?storyId=5400938).

63. *See id*. (referring to the statement of Sen. Cornyn as a proponent of the NSA program).

64. *See id.* (referring to the contrary opinion of the chairman of the Judiciary Committee, Arlen Specter).

65. *See, e.g.*, Solove, *supra* note 13, at 1095–1101.

technologies do not necessarily provide law enforcement with any extrasensory ability—that is, these technologies are arguably just a more efficient substitute for legitimate policing activities like physical surveillance. For example, with enough manpower, police departments could theoretically station officers at every corner of a city and meticulously monitor the movements of every passing person and automobile. Instead, these technologies allow law enforcement to investigate wrongdoing and enforce the law in an astonishingly efficient manner. With minimal manpower, a police department can keep watch on an entire community, document criminal activity, and collect extensive data. As will be discussed in Part II, courts are understandably hesitant to limit the efficiency of law enforcement. The intrusiveness of these technologies has been further enhanced with two ongoing developments in the digitally efficient investigative state that will be discussed in the next two sections: (1) the declining cost and increased feasibility of mass data storage, and (2) the use of data fusion centers to centralize data and improve broad investigative access.

B. The Declining Cost of Data Storage and Mass Recordation

Previously, the potential harms of surveillance technologies were minimal because extensive data storage was both costly and technologically infeasible. But in recent years, technological advances have decreased the cost of data retention and made extensive, high-density data storage possible. Indeed, the "greatest single protector of privacy—amnesia—will soon be a thing of the past."[66] Patricia Bellia has referred to this phenomenon as the move towards perfect memory.[67] Once more, without many regulations on surveillance data retention, law enforcement is arguably incentivized to take advantage of the declining costs of storage by creating "digital dossiers" [68] to aid in future investigations.

At its core, digital technology requires the conversion of data, whether in text, audio, or image form, into a series of binary digits, known as bits.[69] The first IBM hard drive introduced in 1956 stored a mere two-thousand bits per square inch.[70] By 1981, IBM's hard drives could hold twenty MB (or twenty million bits) per square inch and by 2006 that number had risen to one-hundred GB (or one-hundred billion) bits per square inch.[71] Improvements in storage density mean that more information, be it images, text, or video from surveillance technology, can be stored in an extremely small space for little money.

The improvements in efficiency and density of storage without serious regulation serve to incentivize law enforcement to store as much surveillance material as possible. Scholars have suggested that without serious legislative

66. Balkin, *supra* note 10, at 14.
67. Patricia Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 140 (2008).
68. *See generally* Solove, *supra* note 13, at 1067 (defining "digital dossier").
69. Bellia, *supra* note 67, at 142.
70. *Id*. at 143. As a reference point, eight bits is equal to one byte, with a thousand bytes equal to one kilobyte (KB), one million bytes equal to a megabyte (MB), and one billion bytes equal to a gigabyte (GB).
71. *Id*. at 144.

restrictions, the law provides incentives for organizations "to retain data in anticipation of future transactions . . . ."[72] There is little reason to think that law enforcement would be incentivized to purge personal data obtained from surveillance technology if that data could be used in future criminal investigations and the cost of the data retention is minimal. If a person is a suspect in a future crime, data on their previous movement and whereabouts could be invaluable. Furthermore, law enforcement could also use surveillance data to search for potential witnesses of crimes ex post. The improvements in data storage capabilities only increase the potentially pervasive nature of surveillance technologies.

C. Data Fusion and the Move Towards a Centralized Investigative State

Technological progress has facilitated the collection and storage of vast quantities of data by law enforcement. Further, individual departments are highly incentivized to collect as much personal information as possible, since few laws regulate data storage and the cost of retention continues to plummet.[73] But an additional development has further enhanced the capabilities of the digitally efficient investigative state—federal and state investment in criminal data sharing and centralization programs. In 2003, the Department of Justice began the National Criminal Intelligence Sharing Plan (NCISP), which is designed at improving the sharing of criminal intelligence data.[74] Originally, these fusion centers were created by Congress as central databases for compiling terrorist-related information that could be shared with local law enforcement.[75] These fusion centers, though, have been used for the sharing of all kinds of law enforcement information, including "collecting and distributing criminal intelligence of the most mundane kind."[76] The federal government currently operates seventy-two fusion centers around the country, including three major fusion centers near New York City, Los Angeles, and Dallas.[77] Some states, like Maryland, have created their own fusion centers at the state level.[78] Maryland has even begun loading ALPR data into these state fusion centers, allowing the information on an individual's movements to be shared with other law enforcement agencies.[79] There are undoubtedly major criminological benefits to such centralized information sharing. Rather than trying to piece together a coherent picture of a criminal suspect's behavior from disconnected clues, police can turn to a central archive that contains a

72. *Id*. at 152.

73. *See generally id*. (stating that data storage has become increasingly cheap and regulations are the exception rather than the rule).

74. U.S. DEP'T OF JUSTICE. BASELINE CAPABILITIES FOR STATE AND MAJOR URBAN AREA FUSION CENTERS 2 (Sept. 2008), *available at* http://www.it.ojp.gov/documents/baselinecapabilitiesa.pdf.

75. Ken Dilanian, *Security at What Price?*, L.A. TIMES, Nov. 15, 2010, at A8.

76. *Id*.

77. *State and Major Urban Area Fusion Centers*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/files/programs/gc_1156877184684.shtm (last visited Sept. 7, 2011).

78. 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.

79. *Id*.

comprehensive "digital dossier"[80] of all data collected by law enforcement across the country on a given person's movements over many years.

Further complicating the issue, federal fusion centers commonly outsource data collection to private organizations.[81] This use of non-state actors as arbiters of extensive personal information is especially problematic, because the federally-funded fusion centers do not follow uniform protocol or follow uniform regulations on the assemblage of personal records.[82] And the government isn't the only actor attempting to aggregate data from surveillance technologies; private entrepreneurs like the National Vehicle Location Service (NVLS) have thrived in the current regulatory vacuum by aggregating the selling ALPR data.[83] Organizations like NVLS collect license plate data from both public and privately operated ALPR systems. NVLS then makes this data available to all participating law enforcement agencies.[84] Interestingly, NVLS also makes a portion of the data available to private lending institutions and their collection agents to assist in the recovery of collateral.[85] This of course presents a unique legal conundrum. NVLS is not a state actor, but rather is a private company, and thus it is sheltered from certain legal obligations.[86] NVLS serves instead as a third-party intermediary, facilitating the sharing the aggregation of surveillance data between law enforcement agencies and private actors.

The development of government fusion centers represents a growing trend in the digitally efficient investigative state towards information sharing and centralization. This represents, yet again, a massive improvement in policing efficiency. The sharing of information, which once required telephone or in-person communication, can now be accomplished instantly through remote access to centralized catalogues.

In sum, the digitally efficient investigative state has transformed law enforcement. First, new technologies like ALPR and surveillance with facial recognition have made law enforcement far more efficient. Second, the decreasing cost of information storage has made it feasible, and in fact advantageous, for law enforcement to collect and store personal data indiscriminately. And finally, federal fusion centers have facilitated the sharing of this information through centralized databases using private contractors. Despite the enormous powers of the digitally efficient investigative state, the courts have avoided regulating these emerging technological trends, largely for fear of limiting policing efficiency. In the absence of legislative or judicial regulation, the digitally efficient investigative state is radically reshaping social conceptions of privacy. The next section evaluates the constitutionally relevant implications of the digitally efficient investigative state. Given the dearth of empirical work on the specific effects

80. Solove, *supra* note 13, at 1085.
81. Dilanian, *supra* note 75, at A8.
82. *Id*.
83. *National Vehicle Location Service FAQs*, NAT'L VEHICLE LOCATION SERV., http://nvls-lpr.com/nvls/nvls_faq.html?pp=1#ans1 (last visited Sept. 14, 2011).
84. *Id*.
85. *Id*.
86. *Id*.

of the digitally efficient investigative state, I draw on psychological and behavioral studies to demonstrate the potential impact of these new technologies.

D. The Implications of the Digitally Efficient Investigative State

1. Potential Benefits

Before attempting to regulate the digitally efficient investigative state, it is important to understand the potential social benefits of these emerging technologies. First, there is virtually no doubt that the use of surveillance technologies can deter some types of crimes.[87] There is a limited amount of empirical data supporting a correlation between the use of surveillance technologies and decreases in certain types of crime. Research completed by Jennifer King, Deirdre Mulligan, and Steven Rafael found that while surveillance technology may not significantly reduce violent crime, it does substantially deter property crime.[88] This is understandable given the fact that property crime is generally more sensitive to incentives than violent crimes.[89] The authors used San Francisco as a case study to investigate all crimes that occurred within one-thousand feet of nineteen criminal surveillance cameras located within the city limits between 2005 and 2008.[90] The authors found a statistically significant decrease in property crimes of approximately 23% after the installation of the cameras.[91] Other, less empirically controlled measures have also indicated that surveillance tools deter criminality. In Redwood City, California, for example, the installation of surveillance cameras coincided with an 11% drop in all crime near the sights of the installation after one year, and a 33% decrease in the second year.[92] And in Tacoma, Washington, the installation of cameras coincided with a 35% decrease in assaults, trespassing, vandalism, and prostitution.[93] The available empirical evidence, therefore, suggests a strong correlation and likely a causal link between surveillance technologies and some decreases in some criminal activity.[94]

---

87. *See, e.g.*, Jennifer King et al., *Fighting Crime With Publicly-Financed Surveillance Cameras: The San Francisco Experience*, CAL. POL'Y OPTIONS 2009 145, 158, *available at* http://www.spa.ucla.edu/webfiles/doc /116679final.pdf (detailing the results of a study where 19 surveillance cameras were installed and a statistically significant reduction in crime was observed).

88. *Id*.

89. *See* Steven Raphael & Rudolf Winter-Ebmer, *Identifying the Effect of Unemployment on Crime*, 44 J.L. & ECON. 259, 260 (2001) ("To the extent that increased legitimate employment opportunities deter potential offenders from committing crimes. . .with stronger effects for property crime than for violent crime.").

90. King et al., *supra* note 87, at 145–46.

91. *Id.* at 153.

92. Max Guirguis, *Electronic Visual Surveillance and the Reasonable Expectation of Privacy*, 9 J. TECH. L. & POL'Y 143, 148 (2004).

93. *Id.* at 147–48 (citing Bronislaus B. Kush & Emilie Astell, *City Ready for Close-up on Crime–Surveillance Camera to Monitor Downtown*, WORCESTER TELEGRAM & GAZETTE, Aug. 27, 2003, http://docs.newsbank.com/openurl?ctx_ver=z39.88-2004&rft_id=info:sid/iw.newsbank.com:AWNB:WTLB&rft_val_format=info:ofi/fmt:kev:mtx:ctx&rft_dat=0FD4FBAC2A44C12A&svc_dat=InfoWeb:aggregated5&req_dat=0D0CB57DF8A1C275.

94. The empirical studies I referenced utilized different levels of experimental controls. Hence, I stop short of declaring a clear, causal link between surveillance technologies and decreased criminal activity.

In addition, the use of third-party databases such as financial records has been "increasingly useful to law enforcement officials . . . [in] detect[ing] fraud, espionage, fugitives, smuggling cartels, drug distribution rings, and terrorist cells."[95] In terrorist investigations, access to expansive private records has helped law enforcement identify individuals that provide assistance to terrorist groups.[96] These types of records are more common than ever given the technological advancements that permit low-cost, high-density data compilation.[97] Overall, though, there are only a small number of empirical experiments assessing the potential criminological benefits of police surveillance technologies. It may, therefore, be useful to speculate on the potential criminological implications of surveillance technologies by broadly examining behavioral and psychological research. More specifically, research into the phenomenon of deindividuation and deterrence theory bolsters the case, at least theoretically, for police surveillance technology. Deindividuation has been described as the psychological state where, under conditions of anonymity, people become less-self regulated, and thus more likely to commit certain crimes.[98] According to deindividuation theory, a person's "inner restraints are lost when 'individuals are not seen or paid attention to as individuals.'"[99] Later research has shown a clear relationship between anonymity and aggressive, dangerous behavior; if a person believes their identity is unknown, they are more likely to act in reckless, dangerous, or criminal activity.[100] For example, research has shown a relationship between anonymity and aggressive driving behavior,[101] theft,[102] assault,[103] torture,[104] and even killing.[105] One study examining violence in Northern Ireland found a close relationship between anonymity and aggression in interpersonal assaults.[106] There, Andrew Silke evaluated assaults over a thirty-month period, coding information about the attacks including the level of injury, the number of victims, whether the attacker vandalized property, and most importantly, whether the attacker demonstrated any evidence of deindividuation by wearing

95. Solove, *supra* note 13, at 1090.

96. *Id*.

97. *Supra* Part II.

98. Leon Festinger et al., *Some Consequences of De-individuation in a Group*, 47 J. ABNORMAL & SOC. PSYCHOL. 382, 389 (1952).

99. Andrew Silke, *Deindividuation, Anonymity, and Violence: Findings from Northern Ireland*, 143 J. SOC. PSYCHOLOGY 493, 493 (Aug. 2003) (citing Leon Festinger et al., *supra* note 98).

100. *See, e.g.*, Edward Diener et al., *Effects of Deindividuation Variables on Stealing Among Halloween Trick-or-Treaters*, 33 J. PERSONALITY & SOC. PSYCHOL. 178, 178 (1976) (discussing Festinger's findings that "when identification of group members decreased" members were more likely to take part in unacceptable behavior); Patricia A. Ellison et al., *Anonymity and Aggressive Driving Behavior: A Field Study*, 10 J. SOC. BEHAVIOR & PERSONALITY 265, 270–71 (1995) (discussing how the anonymity of being in a vehicle "facilitate[s] aggressive behavior"); Jurgen Rehm et al., *Wearing Uniforms and Aggression: A Field Experiment*, 17 EUROPEAN J. SOC. PSYCHOL. 357, 358 (1987) (stating that "decreased personal identifiability leads to usually proscribed behavior").

101. Ellison et al., *supra* note 100, at 270–71.

102. Diener et al., *supra* note 100, at 182.

103. Silke, *supra* note 99, at 496.

104. Robert I. Watson, Jr., *Investigation Into Deindividuation Using a Cross-Cultural Survey Technique*, 25 J. PERSONALITY & SOC. PSYCH. 342, 343–44 (1973).

105. *Id*. at 343.

106. Silke, *supra* note 99, at 496.

a disguise.[107] Silke found that when the attacker wore a mask or attempted to protect her anonymity, the attack was more severe, more likely to involve multiple victims, and more likely to involve additional vandalism.[108] Similar studies have also uncovered evidence of the deindividuation effect in electronic mediums, like online chat programs.[109] Admittedly, this brief summary of deindividuation takes some liberties in including studies that are quite various and different in salient factual respects. But this broad assessment does suggest that the deindividuation literature could potentially be used to support the use of investigative surveillance technologies as mechanisms utilized to decrease anonymity, thereby lowering the likelihood of criminal activity.

Conversely, there is a cogent argument to be made under classical deterrence theory that long-term, expansive surveillance—like that currently used in the digitally efficient investigative state—would hypothetically dissuade potential wrongdoers. Under the classical psychological theories of deterrence, the motivation for a crime is calculated by subtracting the costs from the potential rewards of the criminal activity.[110] The expected costs include the certainty of punishment, the potential severity of punishment, and the celerity or rapidity of punishment.[111] John Carroll developed one of the first psychological approaches to criminal deterrence in arguing that offenders consider four dimensions when deciding whether or not to commit a crime: (1) the probability of success; (2) the potential rewards; (3) the probability of criminal sanctions; and (4) the severity of sanctions.[112] Put simply, people commit crimes when the motivations for crime are greater than the motivations for non-criminal activities. As the perceived risks of criminal activity increase, the likelihood of a person committing a crime decreases. But Carroll observed that the probability of criminal sanctions was one of the least important variables in the criminal's decision-making process.[113] While the likelihood of punishment is a serious consideration, its effects on the criminal decision-making process should not be overstated. Extensive psychological research has demonstrated that the severity of punishment has little impact on a criminal's likelihood of committing a crime.[114] Nonetheless, substantial

107. *Id*. at 494–96.

108. *Id*. at 496.

109. *See, e.g.*, Adam N. Joinson, *Self-Disclosure in Computer-Mediated Communication: The Role of Self- Awareness and Visual Anonymity*, 31 EUROPEAN J. SOC. PSYCHOL. 177, 182 (2001).

110. *See, e.g.*, John S. Carroll, *A Psychological Approach to Deterrence: The Evaluation of Crime Opportunities*, 36 J. PERSONALITY & SOC. PSYCH. 1512 (Dec. 1978) (proposing that crime is a function of the criminal picking the option with the greatest value).

111. *Id.* at 1513.

112. *Id*.

113. *Id*. at 1516.

114. *See, e.g.*, William C. Bailey & Ruth P. Lott, *Crime, Punishment and Personality: An Examination of the Deterrence Question*, 67 J. CRIM. LAW & CRIMINOLOGY 99, 104–05 (1976) (studying university students' likelihood to commit crimes given the severity and certainty of punishment); Robert F. Meier & Weldon T. Johnson, *Deterrence as Social Control: The Legal and Extralegal Production of Conformity*, 42 AM. SOC. REV. 292, 299–301 (1977) (finding that extralegal influences are more important than controlling influences on use of marijuana); Matthew Silberman, *Toward a Theory of Criminal Deterrence*, 41 AM. SOC. REV. 442, 443 (1976) (analyzing the likelihood of deterrence based on perceived certainty of punishment and conformity to social norms); Gordon P. Waldo & Theodore G. Chiricos, *Perceived Penal Sanctions and Self-Reported Criminality: A Neglected Approach to Deterrence Research*, 19 SOC. PROBS. 522, 529–36 (1972) (looking at

psychological and criminological research has found consistent, but albeit modest, correlations between the perceived certainty of formal sanctions and the likelihood of criminal behavior.[115]

Similar evidence of a psychological link between the perceived likelihood of sanctions and criminal deterrence has been witnessed in the policing context, where obvious visible evidence of policing surveillance decreases the likelihood an individual will commit a traffic violation like speeding.[116] Three psychological deterrent effects have been observed in relation to police surveillance: on-view effects, memory effects, and general halo effects.[117] According to the on-view effect, individuals are less likely to break the law when in direct view of policing surveillance.[118] For example, a person is less likely to run a stop sign or park illegally in direct view of a law enforcement officer. Memory effects are observed when individuals are less likely to engage in illegal behavior in a certain location when they have previously seen police surveillance at that location in the past.[119] Finally, the halo effect describes a person's likelihood to engage in less illegal behavior in general after witnessing the presence of police surveillance; the individual not only avoids illegal behavior in the vicinity where police surveillance is happening or has occurred, but also avoids illegal behavior generally because of the observed surveillance.[120] Under these various deterrence theories, surveillance increases the perceived risk of being caught for a criminal deed and thereby somewhat reduces the likelihood of criminality. "[I]t is intuitively clear" that the likelihood of criminal sanctions "do[es] deter some criminal behavior by some people (as anyone who has ever lightened a foot on a gas pedal after observing a police car in the rear-view mirror can attest)."[121]

Indeed, there is reason to believe that the use of surveillance technologies can decrease criminal activity—if individuals know that they are being monitored regularly by ALPR, surveillance cameras, and facial recognition software, they will be less likely to engage in criminal activity for fear of being identified and apprehended.[122] Given the decreasing costs of these technologies, this revelation has important policy and budgetary consequences. In 2006, the United States spent over $98 billion on policing and over $46 billion on the judiciary.[123] Significant scholarship has focused on the effects of

---

the likelihood of self-reporting of marijuana use and petty theft).

115. *See, e.g.*, Harold G. Grasmick & Herman M. Milligan, Jr., *Deterrence Theory Approach to Socioeconomic/Demographic Correlates of Crime*, 57 SOC. SCI. Q. 608, 609 (1976) (explaining research that shows the correlation between socioeconomic/demographic variables and frequency of law violations incorporated into deterrence theory); Gary F. Jensen, "*Crime Doesn't Pay": Correlates of a Shared Misunderstanding*, 17 SOC. PROBS. 189, 192 (1969) (discussing the correlation between the belief that law breakers are caught and punished and the deterrent effect this belief has).

116. Talib Rothengatter, *The Effects of Police Surveillance and Law Enforcement on Driver Behaviour*, 2 CURRENT PSYCHOL. REV. 349, 351 (1982).

117. *Id*.

118. *Id*.

119. *Id*.

120. *Id*.

121. John Monahan & Elizabeth Loftus, *The Psychology of Law*, 33 ANN. REV. PSYCHOL. 441, 446 (1982).

122. *See generally* Rothengatter, *supra* note 116, at 351–52 (explaining that obtrusive police presence has three effects on individuals and that these effects tend to deter potential criminals from breaking the law).

123. U.S. Bureau of Justice Statistics, *Key Facts at a Glance, Direct Expenditures By Criminal Justice*

various policing tactics on reducing crime, such as incarceration rates[124] and the size of the local police force.[125] Given the available evidence that demonstrates a compelling link between surveillance and decreased criminality, communities would be remiss to not take advantage of some surveillance technologies as a deterrent mechanism.[126]

What remains inconclusive, though, is whether the use of these technologies for mere observational comparison or indiscriminate data retention affects the technology's usefulness as a criminal deterrent. Since individuals are notoriously bad at risk assessment, there may be a strong argument that the technologies serve as a psychological deterrent, whether they merely work as observational comparison tools or as true vehicles for widespread data collection. More psychological research would be helpful in understanding how individuals perceive surveillance technologies, and whether limiting their uses to mere observational comparison would tangibly affect their usefulness as criminal deterrents.

Second, the use of surveillance technologies like ALPR limits police discretion, which may reduce racial or ethnic profiling. At least one study "analyzed computer traffic from police cruisers in a predominantly white suburban town and found that the officers were more likely to run license-plate checks on cars with black drivers than on cars with white drivers . . . ."[127] Even more disturbing, the likelihood an officer would run the license plate of a black driver increased the "farther they were from the border of the neighboring, black-dominated metropolis."[128] The use of ALPR for broad and undifferentiated observational comparison could, conceivably, correct for this kind of implicit bias. Previously police officers had to exercise a significant amount of discretion in deciding which license plates to run through a computerized database. ALPR, by contrast, is efficient enough to run the plates of all nearby automobiles through a computerized database, without making any potentially biased choices. Facial recognition could potentially provide this same benefit as well—rather than relying on officers to make unbiased investigative choices, facial recognition systems of the future may be efficient enough to engage in undifferentiated observational comparison of all surrounding individuals.

Third, aggregated data may serve a useful evidentiary purpose that is not readily apparent at the time of collection. In lauding the benefits of ALPR data retention, the IACP and other law enforcement advocacy groups have noted

---

Function, 1982-2007, OFFICE OF JUSTICE PROGRAMS, http://bjs.ojp.usdoj.gov/content/glance/tables/exptyptab.cfm (last visited Sept. 7, 2011).

124. *See, e.g.*, Steven D. Levitt, *The Effect of Prison Population Size on Crime Rates: Evidence From Prison Overcrowding Litigation*, 111 Q. J. ECON. 319, 339 (1996) (describing how incarceration rates impact the crime rate).

125. *See, e.g.*, Steven D. Levitt, *Using Electoral Cycles in Police Hiring to Estimate the Effect of Police on Crime*, 9283 AMERICAN ECON. REV. 1244, 1247 (1997) (describing how the size of the police force impacts the crime rate).

126. Rothengatter, *supra* note 116, at 351–52.

127. Samuel R. Gross & Debra Livingston, *Racial Profiling Under Attack*, 102 COLUM. L. REV. 1413, 1425 (2002) (citing Albert J. Meehan & Michael Ponder, Race and Place: The Ecology of Racial Profiling African American Motorists 10–11 (2001) (unpublished manuscript, on file with the Columbia Law Review)).

128. *Id.*

that "seemingly irrelevant or untimely information may acquire new significance as an investigation brings new details to light."[129] Consider again the earlier example of a suspected child abduction that occurs near an intersection armed with an ALPR system. If an ALPR system only recorded license plates that matched a hotlist of active offenders, it is unlikely that the system would be of much use in finding witnesses to the child abduction, or finding the license of the suspected abductor. Conversely, if the ALPR system retained data on every passing car, police would instantly have dozens of leads on potential suspects and witnesses.

2. Potential Harms

The unlimited and unregulated use of surveillance technologies, particularly those that collect vast amounts of data, has several potentially dangerous consequences. Again, given the lack of solid, empirical evidence about this subject matter, I extrapolate from psychological and behavioral research to predict possible harmful implications of mass police surveillance. First, there is mounting evidence that law enforcement uses these surveillance tools to target unpopular minorities without particularized suspicion of criminal wrongdoing.[130] In Birmingham, United Kingdom, journalists recently revealed an extensive network of surveillance cameras and ALPR cameras nicknamed "Project Champion," which were being utilized by police to indiscriminately monitor local Muslims with "virtually no consultation, oversight or regard for the law."[131] The project was designed to monitor any individuals entering and leaving a predominantly Muslim suburb.[132] The data was then to be uploaded to regional and national law enforcement databases.[133] Even more disconcerting, police in Birmingham allegedly attempted to conceal the actual purpose of the surveillance cameras and ALPR cameras.[134] Many advocates have expressed concern over similar programs instituted by law enforcement in the United States.[135] The Human Rights Commission claims that Muslims in the San Francisco Bay Area and elsewhere have been subjected to constant surveillance by law enforcement, as part of a broader pattern of racial profiling and discrimination.[136] And there are growing allegations that the FBI targeted Muslim Americans for surveillance simply because of their religious beliefs.[137] Absent legislative regulation, there is a grave risk that police may use these emerging technologies for the dragnet surveillance of unpopular minorities.

---

129. IACP PRIVACY ASSESSMENT, *supra* note 25, at 37 (citing 68 Fed. Reg. 14140 (2003)).
130. Lewis, *supra* note 27.
131. *Id.*
132. *Id.*
133. *Id.*
134. *Id.*
135. Shoshana Walter, *Muslims Reject SFPD Surveillance Program*, THE BAY CITIZEN (Sept. 24, 2010, 4:30 PM), http://www.baycitizen.org/policing/story/san-francisco-muslims-reject-sfpd/.
136. *Id.*
137. *See, e.g.*, Shan Li, *FBI Violated the Rights of Muslims, Lawsuit Alleges*, L.A. TIMES, Feb. 24, 2011, at AA3 (discussing a lawsuit pertaining to an FBI operation that monitored mosque attendees solely on the basis of religion).

Second, the unregulated collection of extensive surveillance data of the innocent increases the likelihood of abuse and corruption. This is a particularly relevant concern to the digitally efficient investigative state, as the unregulated use of ALPR, surveillance cameras, and facial recognition can lend themselves to vast data collection. If nothing else, the collection of extensive personal data may incentivize law enforcement to conduct "fishing expeditions" that directly gainsay the purpose of the Fourth Amendment.[138] At its core, the Fourth Amendment is a tool to "police the police."[139] The Fourth Amendment "positively invites constructions that change with changing circumstances,"[140] but fishing expeditions have consistently and uniformly been viewed as among the most blatant and unreasonable forms of Fourth Amendment violations.[141] With extensively collected personal data, law enforcement can engage in pervasive searches without any particularized suspicion. Daniel Solove has gone as far as to suggest that these fishing expeditions could include automated searches that would exacerbate racism, stereotyping, or profiling.[142] The availability of expansive amounts of personal data can also facilitate the use of that information for other dishonest purposes. It is not implausible that the State could "amass data for use in silencing or attacking enemies, critics, undesirables, or radicals."[143] The Federal Bureau of Investigation's (FBI) use of data collected about Martin Luther King, Jr. serves as a poignant reminder of the potential for law enforcement abuse. Some scholars have suggested that the FBI first investigated King for potential links to communism, but once these ties were discredited, several prominent FBI leaders used the collected data to expose King's private sexual behavior in an effort to discredit and attack his beliefs.[144] President Richard Nixon also notoriously used his powerful political position to collect "embarrassing information to discredit the former Defense Department analyst [Daniel Ellsberg]," and of course "break-in to the Democratic National Committee headquarters in the Watergate office building in Washington, D.C."[145] In addition, the Nixon Administration worked closely with then FBI Director Herbert Hoover to wiretap governmental employees and members of the press deemed to be potential adversaries by the President.[146] The King and Nixon incidents underscore the possibility that law enforcement can selectively and surreptitiously collect information to calumniate critics and political adversaries.[147] The digitally

138. Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse than the Disease*, 68 S. CAL. L. REV. 1, 11 n.45 (1994) (citing LEONARD W. LEVY, ORIGINAL INTENT AND THE FRAMERS' CONSTITUTION 224 (1988)).

139. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 371 (1974).

140. Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 824 (1994).

141. John Shattuck, *In the Shadow of* 1984*: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991, 1002 (1984).

142. *See* Solove, *supra* note 13, at 1109 (stating that automated investigations based on profiles share problems experienced with profiling including inappropriate use of stereotypes, race, and religion).

143. *Id.* at 1112.

144. DAVID J. GARROW, THE FBI AND MARTIN LUTHER KING, JR. 156–157 (1981).

145. ATHAN G. THEOHARIS ET AL., THE FBI: A COMPREHENSIVE REFERENCE GUIDE 76 (1999).

146. *Id.*

147. *See* JOSEPH BENSMAN & ROBERT LILIENFELD, BETWEEN PUBLIC AND PRIVATE: THE LOST BOUNDARIES OF SELF 97 (1979) ("Large-scale organizations tend to invade privacy . . . in order to use the information so gained as a private means to secure its public goals and in part by using managed leaks to

efficient investigative state collects copious amounts of data on individual movement through the use of ALPR, surveillance cameras, and facial recognition. This amplifies concerns that if not properly regulated, the collection of personal surveillance data could present two unique threats of police abuse: the potential for unscrupulous fishing expeditions and the use of data for ulterior, nefarious purposes.

There is also a psychological literature that suggests that surveillance, even in the form of observational comparison, may facilitate law enforcement corruption.[148] Studies have shown that surveillance instigates and encourages entrapment.[149] Psychological research has also demonstrated that surveillance begets perceptions of dishonesty and cheating.[150] When monitoring surveillance technologies, there is evidence that "observers draw unwarranted dispositional inferences not only from actual behavior that could be explained by situational inducements but also from imagined behavior that situational inducements bring to mind."[151] Dale Miller, Brian Staub, and Penny Visser have found that supervisors in charge of monitoring or observing an individual's behavior are likely to have a cynical view of individual honesty; as they witness incidents of dishonesty in their surveillance, supervisors are more likely to view perfectly honest behavior with suspicion.[152] This behavioral research suggests that concerns about law enforcement abuse and fishing expeditions are not merely idle conjecture—completely reasonable and honest behavior, when viewed through the lens of a law enforcement officer trained to be cynical of those under surveillance, may elicit data mining expeditions and other privacy invasions. When law enforcement has access to vast, unregulated surveillance tools like ALPR and facial recognition software, behavioral research suggests that the King and Nixon incident may be the behavioral norm, rather than the exception.

Third, it is important to recognize that surveillance technologies are capable of collecting extensive personal data indiscriminately. Put differently, "[T]he use of modern data mining and processing methods involves the examination of the innocent as well as the suspect to identify patterns of interest for further investigation."[153] Hence, the collection of data on the innocent can lead to a substantially elevated risk of false positives.[154] This has been called the baseline problem.[155] Imagine a situation where law enforcement used an extensive surveillance camera network and facial recognition software to monitor and record pedestrian movements at every

---

reveal private vices of their organizational and personal enemies.").

148. *See generally* John H. Lingle et al., *Surveillance Instigates Entrapment When Violations are Observed, When Personal Involvement is High, and When Sanctions are Severe*, 35 J. PERSONALITY & SOC. PSYCHOL. 419, 419 (1977); Dale T. Miller, et al., *How Surveillance Begets Perceptions of Dishonesty: The Case of the Counterfactual Sinner*, 89 J. PERSONALITY & SOC. PSYCHOL. 117, 117 (2005).

149. *See* Lingle et al., *supra* note 148, at 419 (stating that subjects were more likely to entrap confederates under certain circumstances when surveillance is present).

150. *See* Miller et al., *supra* note 148, at 117 (stating that, when the likelihood of getting caught cheating was high, observers perceived a target who did not cheat as more dishonest than the average target).

151. *Id.* at 117–18.

152. *Id.* at 128.

153. Alan Travis, *Fight Against Terror 'Spells End of Privacy*,' THE GUARDIAN, Feb. 25, 2009, at 1.

154. Ben Goldacre, *Spying on 60 Million People Doesn't Add Up*, THE GUARDIAN, Feb. 28, 2009, at 15.

155. *Id.*

intersection and in every subway car in New York City over the course of several years. By comparing the faces of passing pedestrians to DMV databases, the software was able to positively identify every passing person with a high level of accuracy and digitally document a detailed record of their movements over the course of many years. Now imagine that, through extensive research, law enforcement can identify a certain pattern of movement that is typical of a person involved in organized crime. Imagine this test is extremely accurate in picking out people involved in organized crime, with an accuracy rate of approximately 90%. Using data mining, it is conceivable that law enforcement could search for all persons who fit this unique pattern and use this as a starting point for a broader criminal investigation. On its face, this seems like a reasonably fair and narrowly tailored form of investigation. But when you apply this test to the entire New York City population of over eight million residents, you are likely to get over eight-hundred thousand false positives.[156] The risk of large numbers of false positives "alters the balance of power between the government and the people, exposing individuals to a series of harms, increasing their vulnerability and decreasing the degree of power they exercise over their lives."[157]

Finally, the indiscriminate collection of data may harm a citizen's perceptions of procedural fairness. This may be particularly problematic if digitally efficient investigative technologies are used to indiscriminately collect data on all persons. Without regulation, law enforcement has every motivation to collect as much data as possible when using digitally efficient investigative technologies—both data on suspicious movements by a criminal suspect and data on the everyday movements of innocent individuals. Police are incentivized to engage in undifferentiated data collection, keeping this data in case it may serve a future purpose. It is this collection of data on everyday, seemingly innocent behavior that can irreparably harm a government's relationship with the community and increase public distrust. Individual reactions to computer surveillance represent perhaps the most analogous example of the relationship between perceived privacy violations and perceptions of procedural fairness. Brad Alge conducted a psychological survey on the effects of workplace computer surveillance on employees' perceptions of procedural justice.[158] Alge found that two factors affected an individual's perception of procedural justice in the realm of privacy violations: (1) whether the surveillance was reasonably tailored to only note instances of computer activity that violated company policies, and (2) whether employees felt they had some say in how the surveillance worked.[159] Hence, Alge recommended that employers who are considering the use of software to monitor the computer activities of their employees should seriously consider limiting their monitoring to activities "relevant to their job performance," and that employees should "have input into the electronic monitoring process."[160]

156. *See id*. (explaining the applicability of the baseline problem way in the UK).

157. Solove, *supra* note 13, at 1105.

158. Brad Alge, *Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice*, 86 J. APPLIED PSYCHOL. 797, 797 (2001).

159. *Id*. at 802–03.

160. *Id*. at 803.

A similar lesson can be applied to the indiscriminate collection and centralization of personal data by law enforcement. Such indiscriminate retention, unlike tailored observational comparison, does not limit surveillance to relevant activities like those that elicit suspicion of criminal wrongdoing. Instead, indiscriminate data collection entails the recording of all types of data, both relevant to ongoing investigations and irrelevant to immediate policing purposes. Psychologically, this kind of surveillance is highly likely to decrease individuals' feelings of procedural fairness and trust. And since there has been little legislative action to regulate this type of data collection, individuals are likely to feel as if they have minimal input in the monitoring process.

The possible harms of the digitally efficient investigative state are real and constitutionally significant. The next Part analyzes the current judicial doctrine on the constitutionality of law enforcements' warrantless use of investigative surveillance technologies. Despite the serious concerns raised by unregulated surveillance data retention, the current Fourth Amendment doctrine provides few avenues for judicial relief.

III. THE FOURTH AMENDMENT AND SURVEILLANCE TECHNOLOGIES

The Fourth Amendment protects against unreasonable searches and seizures.[161] The Supreme Court has interpreted this Amendment to mean that warrantless searches are presumptively unreasonable, with several notable exceptions.[162] But in order to be covered by the Fourth Amendment, a police action must be deemed a search under the meaning of the Fourth Amendment.[163] This Part will begin by analyzing the Court's definition of the term search when applied to surveillance technologies. Next, I explain the underlying distinction between technologies that improve efficiency and those that increase intrusiveness. This distinction seems to hold particular importance in the burgeoning constitutional doctrine of emerging surveillance technologies.

A. Defining a Search

The Court has never provided a single, consistent definition of the term "search." Indeed, the Supreme Court has executed its interpretation of the Fourth Amendment "in an erratic and often contradictory manner."[164] The Court's understanding of the Fourth Amendment has evolved in response to emerging surveillance technologies. Originally the Court argued that a search required a physical invasion by the government.[165] But this doctrine was incongruent with the invasive surveillance techniques used by law enforcement—after all, surveillance technologies like wiretapping rarely

161. U.S. CONST. amend. IV.
162. Johnson v. United States, 333 U.S. 10, 13–14 (1948).
163. United States v. Karo, 468 U.S. 705, 712 (1984).
164. BRADFORD P. WILSON, ENFORCING THE FOURTH AMENDMENT: A JURISPRUDENTIAL HISTORY 4 (Harold Hyman & Stuart Bruchey eds., 1986).
165. Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled by* Katz v. United States, 389 U.S. 347, 352–53 (1967).

involve a physical invasion.[166] Since 1967, the Court's definition of search has been focused on a two-part test announced in *United States v. Katz* that weighs a person's subjective expectation of privacy and whether society recognizes that expectation as objectively reasonable.[167]

The Court first analyzed the constitutionality of surveillance technologies under the Fourth Amendment in *Olmstead v. United States*.[168] The trial court convicted the defendants in *Olmstead* of organizing a conspiracy to import and sell liquor in violation of the National Prohibition Act.[169] Federal prohibition officers intercepted incriminating statements made by the defendants during telephone conversations.[170] The prohibition officers had inserted several small wires "along the ordinary telephone wires from the residences of four of the petitioners . . . . The insertions were made without trespass upon any property of the defendants."[171] In total, the prohibition officers listened to the defendants' telephone conversations for many months before collecting the necessary evidence for an arrest and conviction.[172] The Court upheld the constitutionality of the warrantless wiretapping of the defendants.[173] In reaching their conclusion, the Court stressed the difference between mere wiretapping and real, physical intrusion.[174] Wiretapping involves no physical intrusion into a person's home or seizure of her tangible, physical effects, making it constitutionally different according to the *Olmstead* Court.[175] The Court also compared the tapping of phone lines outside of the home to the searching of a public highway.[176] As a result, *Olmstead* "recognized a new constitutional threshold for Fourth Amendment protection—tangible physical intrusion by the government."[177]

This constitutional threshold was later reaffirmed in *Goldman v. United States*.[178] There, too, law enforcement surreptitiously listened to a private conversation.[179] Using a device called a detectaphone, the police were able to listen to the defendant's conversation through an adjoining wall.[180] The defendant attempted to distinguish his case from *Olmstead*.[181] But unlike Olmstead, the defendant never communicated his conversation over a so-called public highway like a telephone wire; the speaker never "project[ed] his voice beyond the confines of his home or office," and as a result, never seemed to assume "the risk that his message may be intercepted."[182] But the Court was

166. *Katz*, 389 U.S. at 352–53.
167. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 211 (1986).
168. *Olmstead*, 277 U.S. at 465–66.
169. *Id.* at 455.
170. *Id.* at 456–57.
171. *Id.* at 457.
172. *Id.* at 457.
173. *Id.* at 464.
174. *See id.* at 465–66 (discouraging the enlargement of the Fourth Amendment's language).
175. *Id.* at 466.
176. *See id.* at 465 ("The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.").
177. Hutchins, *supra* note 5, at 424.
178. Goldman v. United States, 316 U.S. 129, 135–36 (1942).
179. *Id.* at 131–32.
180. *Id.*
181. *Id.* at 135.
182. *Id.*

unreceptive to this seemingly logical distinction, and instead rigidly enforced the physical invasion standard from *Olmstead*.[183]

The *Olmstead* standard remained intact for forty years until the Court finally reevaluated the subject in *Katz v. United States* in 1967.[184] The facts in *Katz* were relatively similar to those in the original *Olmstead* case. The defendant was a gambler who used a public telephone booth to place illegal gambling bets.[185] Police affixed a listening device to a public telephone and recorded six of Katz's telephone calls.[186] Using these recorded statements, Katz was convicted at trial.[187] Katz appealed his conviction, arguing that the police actions amounted to a violation of the Fourth Amendment.[188] Rather than reaffirming the *Olmstead* decision, the Court made a dramatic departure from established precedent and held that the Fourth Amendment "cannot turn upon the presence or absence of a physical intrusion . . . ."[189] The Fourth Amendment protects people, not places, from unreasonable searches and seizures.[190] And when a person enters a phone booth and closes the door, the Court determined that it was safe to assume that the person expects her words will not be "broadcast to the world."[191] As a result, the Court held that law enforcement needed to secure a warrant before using wiretapping technology on a person in a public phone booth.[192]

Perhaps the most significant constitutional development from the *Katz* case, though, was tucked away in Justice Harlan's concurring opinion. Justice Harlan laid out an explicit two-part test to determine if law enforcement activity constitutes a search under the Fourth Amendment: "[F]irst that person have exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[193] Harlan's two-prong test has become the de facto standard for determining whether a search has occurred.[194] Hence, when analyzing the application of the Fourth Amendment to emerging technologies, courts begin by applying the two-prong test explicated in *Katz*.

B. The Distinction Between Efficiency and Intrusiveness

In the particular realm of investigative technologies, the courts have also created a formal dichotomy between technologies that merely improve the efficiency of legal investigations, and technologies that increase intrusiveness by giving law enforcement an additional, extrasensory ability. The former

183. *Id.* at 135–36.
184. Katz v. United States, 389 U.S. 347, 512 (1967).
185. *Id.* at 354–355 n.14.
186. *Id.*
187. *Id.* at 348.
188. *Id.* at 348–49.
189. *Id.* at 353.
190. *Id.*
191. *Id.* at 352.
192. *Id.* at 359.
193. *Id.* at 361 (Harlan, J., concurring).
194. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 211 (1986) (applying Justice Harlan's two-prong test and finding no Fourth Amendment violation when the government observed marijuana plants using aircraft over a residence).

technologies are presumptively constitutional and require no warrant,[195] while the latter technologies are viewed with suspicion and required a warrant before use.[196] This section will clarify the distinction between efficiency and intrusiveness under the current doctrine, and give substantive examples of technologies that fall under each category.

To begin with, law enforcement need not obtain a warrant before using surveillance technologies that merely improve the efficiency of otherwise legal investigative techniques.[197] Scholars and courts have described this subset of technologies in various ways: sense-augmenting surveillance,[198] mere substitutes for legal investigations,[199] or simple improvements in efficiency.[200] In *United States v. Knotts*, for instance, the Court upheld the warrantless use of a beeper used by law enforcement to track the movements of a criminal suspect.[201] The defendant in *Knotts* was suspected of purchasing chemicals used for the manufacture of illegal substances.[202] The investigating officers, with the consent of a chemical company, installed a beeper inside of a chloroform container that was sold to the defendant.[203] Law enforcement then used a radio receiver to pick up a periodic signal emitted by the beeper.[204] The police attempted to follow the defendant manually, but they lost track of the defendant after he made "evasive maneuvers."[205] Nonetheless, with the help of the signals emitted from the beeper, law enforcement was able to track the defendant's location over the next three days and secure a search warrant for the defendant's house based upon his suspicious movements.[206] This subsequent search uncovered an extensive methamphetamine laboratory, leading to the defendant's arrest and conviction.[207] The defendant challenged his conviction, arguing that the use and monitoring of the beeper violated his reasonable expectation of privacy.[208] The Supreme Court disagreed and upheld his conviction.[209]

In reaching its conclusion, the Court stressed the suspect's diminished expectation to privacy in an automobile on a public thoroughfare.[210] The Court has always permitted law enforcement to visually observe the movements of

195. *See, e.g.*, United States v. Ishmael, 48 F.3d 850, 855 (5th Cir. 1995) ("While technology certainly gives law enforcement a leg up on crime, the Supreme Court has never equated police efficiency with unconstitutionality." (citation omitted)).

196. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) (explaining that the use of "sense-enhancing technology" to conduct a search that would result in intrusion into a constitutionally protected area is unconstitutional).

197. *See* United States v. Knotts, 460 U.S. 276, 282 (1983) ("Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.").

198. Hutchins, *supra* note 5, at 433.

199. United States v. Pineda-Moreno, 591 F.3d 1212, 1216 (9th Cir. 2009).

200. *Id*.

201. *Knotts*, 460 U.S. at 276.

202. *Id*. at 278.

203. *Id*.

204. *Id*.

205. *Id*.

206. *Id*. at 278–79.

207. *Id*. at 279.

208. *Id*.

209. *Id*. at 280.

210. *Id*. at 281.

individuals on public highways without a warrant.[211] The movements and whereabouts of the defendant could have potentially been uncovered solely through visual observation.[212] Hence, the Court determined that "[t]he fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of [the defendant's] automobile to the police receiver, does not alter the situation."[213] The Court stressed that the use of sense-augmenting technologies has never been deemed unconstitutional.[214] Implicit within the Court's rationale is a hesitancy to inhibit the efficiency of police investigations: "We have never equated police efficiency with unconstitutionality, and we decline to do so now."[215] Hence, *Knotts* has long stood for the proposition that improvements in investigative efficiency do not implicate privacy concerns, nor amount to a search under the Fourth Amendment. The courts have reached similar conclusions in the case of other investigative or surveillance technology like pen registers,[216] GPS surveillance,[217] and recording devices used for voluntary conversations with government agencies.[218]

Throughout these cases, scholars and courts have also stressed the public policy implications of a rule permitting the warrantless use of efficiency-enhancing technologies. The meaning of the Fourth Amendment, according to various courts, "must change to keep pace with the march of science."[219] On the most fundamental level, the way that courts define the constitutional boundaries of the Fourth Amendment reflects a basic social understanding about the proper balance between privacy and safety.[220] As Judge Posner posited in *Garcia*, "There is a tradeoff between security and privacy, and often it favors security."[221] Once more, the test that the courts use must be understood and applied by law enforcement. Orin Kerr has argued that police need clear rules; cases that stray from the *Knotts* standard create confusion and hinder investigators.[222] Despite some variation among a handful of state courts and federal circuits,[223]courts have generally held that technologies that only improve efficiency of investigations do not require a warrant.[224]

The Court has sharply distinguished efficiency-improving technologies from those technologies that give law enforcement an additional, extrasensory ability. According to the Court, law enforcement must obtain a warrant before

211. *E.g.*, *id*. at 282 (citing Hester v. United States, 333 U.S. 10, 14 (1924)).
212. *Id*.
213. *Id*.
214. *Id*.
215. *Id*. at 284.
216. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding constitutional the warrantless use of pen registers to record the telephone numbers dialed by a criminal suspect).
217. *See, e.g.*, United States v. Pineda-Moreno, 591 F.3d 1212, 1215–17 (9th Cir. 2009); United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007).
218. *See* United States v. Caceres, 440 U.S. 741, 750–51 (1979).
219. *Garcia*, 474 F.3d at 997.
220. *See id*. at 998.
221. *Id*.
222. Charlie Savage, *Judges Divided over Rising GPS Surveillance*, N.Y. TIMES, Aug. 14, 2010, at A12.
223. *See id*.
224. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 282–84 (1983) (discussing technologies which require warrants and technologies that do not).

using these technologies.[225] The most prominent case dealing with such a technology is *United States v. Kyllo*, where the Court invalidated the warrantless use of a thermal imaging device on a suspect's home.[226] Law enforcement suspected the defendant of growing marijuana in his home, which likely involved the use of high-intensity lamps generating substantial heat.[227] While sitting in a police car across from the defendant's house, law enforcement used the advanced heat-sensing technology to scan the defendant's home and produce an image of the inside of the house displaying the relative temperatures.[228] The scan showed that the garage area of the defendant's home was substantially warmer than the rest of the house, and substantially warmer than neighboring homes.[229] Using this information, law enforcement secured a warrant and discovered incriminating evidence of marijuana production in the defendant's garage.[230] The defendant challenged his conviction based on the intrusiveness of the thermal imaging device.[231] In finding that the use of thermal imaging amounted to a search, the Court argued that the surveillance was capable of exploring the "details of the home that would previously have been unknowable without physical intrusion . . . ."[232] Perhaps most compelling, the dissenting justices attempted to categorize thermal imaging as merely a sense augmenting technology. "[T]he ordinary use of the senses might enable a neighbor or passerby to notice the heat emanating from a building. . . ."[233] Scholars have argued that the *Kyllo* case is an example of the overly formalistic application of the dichotomy between efficiency and pervasiveness.[234]

But as of today, this explicit dichotomy between efficiency-improving technologies on one hand, and technologies that give law enforcement an intrusive, extrasensory ability on the other, remains the dominant common law principle.[235] The Court has nonetheless acknowledged the importance of quantity as a moderating agent in "temper[ing], at the margins, the Court's unconditional application of the general rules stated above."[236] For example, the Court has acknowledged that highly sophisticated surveillance equipment might be constitutionally proscribed absent a warrant.[237] Circuit courts have reflected this uncertainty with increasingly sophisticated surveillance technologies.[238] The Seventh Circuit aptly explained, "Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier

225. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001).
226. *Id*.
227. *Id*. at 29.
228. *Id*. at 29–30.
229. *Id*. at 30.
230. *Id*.
231. *Id*.
232. *Id*. at 40.
233. *Id*. at 43 (Stevens, J., dissenting).
234. Hutchins, *supra* note 5, at 437.
235. *Id*. at 449 ("Implicitly referencing the two categories of technology identified to date by the Supreme Court—extrasensory and sense augmenting . . . .").
236. *Id*. at 438.
237. Dow Chem. Co. v. United States, 476 U.S. 227, 228 (1986).
238. *See generally* United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) (ruling that when police placed a GPS device on defendant's car without a warrant they did not violate the Fourth Amendment).

times would have been prohibitively expensive."[239] In total, the courts continue to recognize the formal distinction between efficiency and intrusiveness, but the advent of new technologies demands a new constitutional standard. The next Part applies the present doctrine to the digitally efficient investigative state, demonstrating the possible shortcomings of the current standard.

IV. APPLYING THE EXISTING FOURTH AMENDMENT DOCTRINE TO THE DIGITALLY EFFICIENT INVESTIGATIVE STATE

This Part analyzes the constitutionality of the warrantless use of emerging technologies employed in today's digitally efficient investigative state. In particular, I focus on surveillance cameras with facial recognition, ALPR, and third-party databases. In total, I argue that under the current Fourth Amendment doctrine, the warrantless use of surveillance technologies probably does not amount to a search. These technologies do not provide officers with any extrasensory abilities, but merely improve the efficiency of law enforcement investigations. Additionally, these technologies do not interfere with any reasonable expectation of privacy on public thoroughfares. I argue that this demonstrates a need for the Court to rethink the current Fourth Amendment doctrine to account for the possibility of mass surveillance. Such a major doctrinal shift may be imminent, as the Court has already granted certiorari to a controversial surveillance case, *United States v. Jones*,[240] involving the warrantless installation of a GPS device. The Court's pending decision in this case could have major implications for the judiciary's future willingness to regulate surveillance technologies.

A. Warrantless Use of ALPR is Likely Constitutional

Under the current doctrine, ALPR does not appear to be a search based on the meaning of the Fourth Amendment. When weighing ALPR under the *Katz* test, there is serious doubt as to whether a person has a subjectively or objectively reasonable expectation to privacy in her movements on a public highway. Further, there is a strong argument that ALPR merely improves efficiency without tangibly altering the sensory abilities of law enforcement. Overall, it seems improbable that the courts would deem ALPR a search under the Fourth Amendment. I argue that this demonstrates a fundamental disconnect between Fourth Amendment doctrine and the values underlying the Fourth Amendment, which ought to be remedied by judicial action.

First, it seems unlikely that a court would recognize either a subjectively or objectively reasonable expectation of privacy on a public thoroughfare as presently required by *Katz*. When driving a car on public highways, a person is in a public space where "access [is] not meaningfully restricted"[241] and her

239. *Id*. at 998.
240. United States v. Jones, 131 S. Ct. 3064 (2011).
241. Cardwell v. Lewis, 417 U.S. 583, 593 (1974).

appearance is "visible to the public."[242] The Court has held that people have no reasonable expectation to privacy in such public spaces, because "the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public."[243] Under the first prong of *Katz*, it is highly improbable that a person could demonstrate a subjective intent to keep their movements on public highways private. Generally, courts examine this first prong of *Katz* by asking whether a defendant exhibited behavior that suggested a personal desire for privacy. For example, in *California v. Ciraolo*, the police received a tip that a local resident was growing marijuana in his backyard.[244] When the police arrived, they found that the defendant had erected two fences around his property.[245] Rather than securing a warrant, the police used a small plane to fly over and photograph the defendant's property.[246] The police then used these photographs to secure a warrant to further search the property and later arrest the defendant.[247] The Court began its analysis of this case by asking whether the defendant had a subjective expectation of privacy under the *Katz* standard.[248] Despite the fact that the defendant had erected a ten-foot fence around the entire perimeter of his property, the Court concluded that this was inconclusive about whether he truly "manifested a subjective expectation of privacy from *all* observations of his backyard."[249] The Court went as far as suggesting that since a person could possibly see over the fence if "perched on the top of a truck," the defendant's subjective expectation of privacy may be unclear.[250] The defendant in *Ciraolo* almost certainly demonstrated an unequivocal desire to prevent observation of his back yard. And yet the Court was still unconvinced that this qualified as a true, subjective expectation of privacy.[251] It therefore seems highly unlikely that a court would find that a person has a personal expectation to privacy in their movements on a public highway. After all, every time a person enters a public highway, his actions are visible to police officers, traffic cameras, tollbooth surveillance, and all other persons on the thoroughfare.

The next question under the *Katz* test is whether a suspect's expectation of privacy would be recognized by society as objectively reasonable.[252] The Court has given this second prong more weight in the totality of the analysis.[253] The definition of "objective" and "reasonable" are generally vague in the available constitutional doctrine. The Court has used several factors to judge whether a subjective expectation is objectively reasonable, such as whether the

242. United States v. Santana, 427 U.S. 38, 42 (1976).
243. Guirguis, *supra* note 92, at 155 (quoting California v. Greenwood, 486 U.S. 35, 41 (1988)).
244. California v. Ciraolo, 476 U.S. 207, 209 (1986).
245. *Id*.
246. *Id*.
247. *Id.* at 209–10.
248. *Id*. at 211.
249. *Id*. at 211–12.
250. *Id*.
251. *Id.*
252. *Id.* at 211.
253. Hudson v. Palmer, 468 U.S. 517, 525 n.7 (1983).

police activity would have been offensive to the Framers,[254] whether the observation was made in plain sight,[255] and the relative intrusiveness of the tactic.[256] The latter factor, the relative intrusiveness, has been the source of notable scholarship, but remains haphazard and "asymmetrical."[257] Thus, in order to prove that ALPR amounts to a search, a defendant would need to show that there is either a socially reasonable expectation of privacy, or that the relative intrusiveness of ALPR demands some protection. ALPR probably does not fall into either of these categories. First, state and local governments often fund the installation and use of ALPR, much like they fund the use of traffic cameras or tollbooth cameras. The funding and use of ALPR by local law enforcement, therefore, could amount to a value judgment by the community—a judgment that places greater weight on the efficiency gained by the use of ALPR over any potential privacy concerns. Second, the limited case law on advanced surveillance technologies cuts against any ALPR opponents. For example, in *Smith v. Maryland*, the Court found that the warrantless installation of a pen register on a telephone, used to record the numbers dialed from a particular phone, did not amount to a search under the Fourth Amendment.[258] The Court in *Smith* engaged in a *Katz* analysis, asking whether a person had an objectively reasonable expectation to privacy in the phone numbers he dialed.[259] The Court stressed that telephone companies already kept records of the numbers dialed in order to calculate phone bills.[260] As a result, the defendant could not harbor any objectively reasonable expectation of "privacy in information he voluntarily turn[ed] over to third parties."[261] The defendant assumed the risk of others observing the telephone numbers he dialed since the information was available to third parties.[262]

This basic premise has been expanded to public thoroughfares in *Knotts*.[263] When assessing whether the suspect had a legitimate expectation to privacy, the Court bluntly concluded:

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.[264]

---

254. Rakas v. Illinois, 439 U.S. 128, 152–53 (1978) (Powell, J., concurring).

255. *See, e.g.*, United States v. Kim, 415 F. Supp. 1252, 1254 (D. Haw. 1976) (considering whether telescopic surveillance constitutes plain view).

256. Hutchins, *supra* note 5, at 431–32.

257. *Id.*

258. Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

259. *Id.* at 741–42.

260. *Id.* at 742.

261. *Id.* at 743–44.

262. *Id*. Congress has passed a statute that explicitly requires federal law enforcement to get a warrant before using pen registers. 18 U.S.C. § 3121 (2006). But the Court has upheld the basic premise that when a person makes information or behavior viewable to third parties, she likely has no objectively reasonable expectation to privacy. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 285 (1983).

263. *Knotts*, 460 U.S. at 281–82.

264. *Id.*

The Supreme Court's staunch position has been unwavering, suggesting that there is no legitimate, objectively reasonable expectation to privacy in one's movements on public roads.[265]

Second, ALPR does not give law enforcement any extrasensory ability nor does it intrude into the home. ALPR merely improves law enforcement's ability to visually observe the license plates of nearby automobiles in public. ALPR can be easily contrasted with the unconstitutionally intrusive technology condemned in *Kyllo*. There, the Court set a clear standard for the warrantless use of emerging technologies—"obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area'" constitutes a search.[266] The Court in *Kyllo* therefore gave special attention not just to whether the technology enhances the senses of the law enforcement agent, but also to whether it intruded a constitutionally protected area like the home.[267] By contrast, in *Dow Chemical Co. v. United States*, the Court upheld the Environmental Protection Agency's (EPA) warrantless use of advanced aerial photography of a business complex.[268] The technology employed by the EPA was so advanced, in fact, that it could detect "wires as small as 1/2-inch in diameter."[269] Nonetheless, the Court found the warrantless use of this advanced aerial photography to be constitutional, since it did not "penetrate walls or windows as to hear and record confidential discussions,"[270] and the business complex "[did] not share the Fourth Amendment sanctity of the home."[271] Under *Dow*, even technologies that substantially improve an officer's senses are completely constitutional. And the Court rarely scrutinizes the warrantless use of these technologies, so long as they are not used in a way that intrudes on the "sanctity of the home."[272] Using this established case law, there is little doubt that the warrantless compilation of data under ALPR would be constitutional, as it neither intrudes on the home nor gives law enforcement any special, extrasensory ability.

Third, the actual compilation or retention of extensive data using ALPR does not appear to implicate any particular concern under Fourth Amendment doctrine, as demonstrated by *Smith*. Again, the Court held in *Smith* that warrantless access to pen registers raises no Fourth Amendment concerns.[273] After all, a person ought to understand that her phone company may collect a

265. *See also* Rakas v. Illinois, 439 U.S. 128, 153–54 (1978) (Powell, J., concurring) (contrasting reasonable expectations of privacy within one's automobile with expectations of privacy in other locations); South Dakota v. Opperman, 428 U.S. 364, 367 (1976) (describing the logical foundation for the distinction between privacy expectations in automobiles and privacy expectations in other locations); Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (noting that a person has a lesser expectation to privacy in a car because "occupants and its contents are in plain view").

266. Kyllo v. United States, 533 U.S. 27, 28 (2001) (*quoting* Silverman v. United States, 365 U.S. 505, 512 (1961)).

267. *Id*.

268. Dow Chem. Co. v. U.S., 476 U.S. 227, 239 (1986).

269. *Id*. at 238.

270. *Id*. at 239.

271. *Kyllo*, 533 U.S. at 37.

272. *Id*.

273. Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

record of all the phone numbers she dials.[274] She voluntarily turns over this information to the phone company, who she can reasonably expect may convey this information to others.[275] Thus, she has no reasonable expectation to privacy in a list of these numbers.[276] The Court seemed to afford no constitutional significance to the fact that a pen register may, through compiling vast amounts of data on a person, be particularly intrusive.[277] The Court has bluntly cautioned that it is "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[278] Using this doctrinal basis, it seems unlikely that the compilation of extensive data through ALPR systems implicates any special constitutional doctrine. As in *Smith*, a person traveling in a community that utilizes ALPR should reasonably expect that their license plates may be read by advanced technologies and recorded into a database.[279] Every time that a person gets in an automobile, they assume the risk that law enforcement may document their movements.[280] Thus *Smith* only strengthens the constitutional argument for the warrantless use of ALPR for observational comparison and indiscriminate information collection. Overall, it is unlikely that the Court would find the warrantless use of ALPR to be unconstitutional, at least under current doctrine.

B. Warrantless Use of Video Surveillance with Facial Recognition is Likely Constitutional

Similarly, the use of surveillance cameras generally does not amount to a search under the Fourth Amendment. Admittedly, the courts have shown skepticism towards law enforcement's use of surveillance cameras except in circumstances of extraordinary need.[281] Courts have described the use of hidden video surveillance in particular as "one of the most intrusive investigative mechanisms available to law enforcement."[282] But despite claims that the use of video surveillance must be tailored to only times of special necessity, the courts have nonetheless generally permitted the use of video surveillance in public spaces like parks and traffic corners.[283] Courts have retreated back to the *Katz* test in finding that a criminal suspect has no

274. *Id*. at 743–44.

275. *Id*.

276. *Id*.

277. *See id.* at 745 (refusing to differentiate between calls phone company did and did not record). *See also id.* at 747 (Stewart, J., dissenting) (arguing pen register information deserves constitutional protection).

278. Whalen v. Roe, 429 U.S. 589, 605 (1977).

279. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (finding no reasonable expectation of privacy in the telephone numbers an individual calls).

280. *See id*. at 744 (making special note of whether a defendant "assumed the risk").

281. United States v. Nerber, 222 F.3d 597, 603–04 (9th Cir. 2000). *See also* United States v. Mesa-Rincon, 911 F.2d 1433, 1443 (10th Cir. 1990) ("Because of the invasive nature of video surveillance, the government's showing of necessity must be very high to justify its use."); United States v. Torres, 751 F.2d 875, 882 (7th Cir. 1984) ("We think it . . . unarguable that television surveillance is exceedingly intrusive, especially in combination (as here) with audio surveillance, and inherently indiscriminate, and that it could be grossly abused—to eliminate personal privacy as understood in modern Western nations.").

282. *Nerber*, 222 F.3d at 603.

283. *See, e.g.*, United States v. McIver, 186 F.3d 1119, 1125 (9th Cir. 1999).

reasonable expectation to privacy in their movements in a public place.[284] Once more, courts have stressed that video surveillance in public space only amounts to a more cost-effective version of otherwise constitutional visual observation.[285] Using facial recognition with video surveillance, either for observational comparison or data collection purposes, does not appear to implicate any additional constitutional concerns under the current doctrine. Thus, the warrantless use of video surveillance with facial recognition in public space is likely constitutionally permissible under the Fourth Amendment.

First, the *Katz* test has historically been used to uphold the validity of warrantless video surveillance in public. In *United States v. McIver*, for example, the Ninth Circuit held that the warrantless use of video surveillance in a national forest was presumptively constitutional.[286] In *McIver*, the National Park Service suspected that the defendants were growing marijuana on public land.[287] But the Park Service only had ten officers available for surveillance; it was deemed impractical to constantly monitor the suspected area.[288] So the Park Service installed unmanned, motion-activated video surveillance cameras to photograph and record the area continuously.[289] Using the video and photographs collected through the use of this video surveillance, the Park Service was able to assemble incriminating evidence that led to the conviction of the defendants.[290] The defendants challenged their conviction by arguing that the placement of surveillance cameras amounted to a search and thus required a warrant.[291] The Ninth Circuit began its analysis by referring back to the *Katz* test and asking whether the suspects had a subjectively and objectively reasonable expectation to privacy in their actions on public land.[292] Since their actions were done on public property, the Ninth Circuit concluded that "they knowingly exposed their illegal activities to any person who visited that area."[293] Further, the court quickly dismissed the defendants' allegation that the use of video surveillance was an unreasonable search, since "it is also beyond dispute that the Forest Service could have stationed officers to conduct a 24-hour surveillance . . . ."[294] On the whole, the *McIver* case represents the general doctrinal path taken by courts that have considered public video surveillance—when a person is on public land, she loses her reasonable expectation of privacy in her actions.[295]

Second, the Court has resisted categorizing emerging technologies "aimed at simple visual observations from a public place" as constituting a

284. *See, e.g.*, *id*.

285. *See, e.g.*, *id*. ("We reject the notion that the visual observation of the site became unconstitutional merely because law enforcement chose to use a more cost-effective 'mechanical eye' to continue the surveillance.").

286. *Id*. at 1125.

287. *Id*. at 1122.

288. *Id*.

289. *Id*. at 1122–23.

290. *Id*. at 1124.

291. *Id*.

292. *Id*. at 1125.

293. *Id*.

294. *Id*.

295. *Id*. (emphasizing that the surveillance area was open to the public).

search under the Fourth Amendment.[296] In *Ciraolo*, the dissent argued that the use of aerial surveillance of a suspect's backyard amounted to a search under Justice Harlan's language in *Katz*.[297] In the dissent, Justice Harlan was particularly concerned with the evolution of technology, which could result in pervasive searches under the Fourth Amendment that were not necessarily *physically* intrusive.[298] The dissent argued that aerial surveillance amounted to a pervasive search even if it was not physically intrusive.[299] But the majority in *Ciraolo* rejected this logic. *Katz*, according to the majority, protected specifically against the interception of private conversations.[300] In this way, the Court has significantly limited the expansion of *Katz* protections to emerging technologies like video surveillance. Additionally, video surveillance falls within the category of sense-enhancing, not extrasensory technologies. As a result, video surveillance merely improves law enforcement efficiency, without adding any additional, pervasive elements. As already discussed, this suggests that public video surveillance would not require a warrant.

Facial recognition software has also received no special consideration from the Court. A person has no reasonable expectation of privacy in their physical characteristics, such as their voice, handwriting, or facial features.[301] As the Court has already noted, "No person can have a reasonable expectation that others will not know the sound of his voice any more than he can reasonably expect that his face will be a mystery to the world."[302] Even the indiscriminate data retention capability of facial recognition software appears to have no constitutional significance according to the Court's doctrine.[303] While some may argue that facial recognition provides officers with an intrusive, extrasensory ability, it seems to fall well short of the *Kyllo* test and may ultimately serve as an efficient substitute for manual visual comparison. Indeed, the preponderance of case law still suggests that video surveillance with facial recognition is presumptively constitutional: "'[W]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.'"[304]

C. Warrantless Use of Third-Party Databases is Likely Constitutional

The use of third-party databases, which are voluntarily released to law enforcement to assist in criminal investigations, is constitutional. On this issue, the Court has been clear and explicit—the Court has consistently held that a person has no reasonable expectation to privacy in information

296. California v. Ciraolo, 476 U.S. 207, 214 (1986).
297. *Id.* at 218–20, 223 (Powell, J., dissenting).
298. *Id.* at 218.
299. *Id.*
300. *Id.* at 214 (majority opinion).
301. United States v. Dionisio, 410 U.S. 1, 14 (1973).
302. *Id.*
303. *See* Whalen v. Roe, 429 U.S. 589, 605 (1977) (stating that the right to collect data for public purposes is accompanied by a duty to avoid unwarranted disclosures).
304. United States v. Miller, 425 U.S. 435, 442 (1976) (quoting Katz v. United States, 389 U.S. 347, 351).

voluntarily handed over to a third-party.[305] The Court has applied this holding to phone records,[306] bank records,[307] and other instances where a person failed to exhibit a "legitimate expectation of privacy"[308] or "assumed the risk that the company would reveal . . . [the information] . . . to the police . . . ."[309] In total, it appears that ALPR, video surveillance with facial recognition, and third-party databases are constitutional under the current doctrine. I believe this underscores a fundamental inadequacy of the current doctrine—the Court's failure to recognize the privacy concerns implicated by extensive data collection.

D. Jones *as a Test Case for the Constitutionality of the Digitally Investigative State*

While the preponderance of available doctrine suggests that digitally efficient investigative technologies and data retention fit comfortably within constitutional boundaries, a pending case in the Supreme Court, *Jones*, may represent a forthcoming doctrinal shift. *Jones* originates from a Department of Justice request for certiorari on a case out of the Court of Appeals of the District of Columbia, *United States* v. *Maynard*.[310] There, police installed a GPS device on Antoine Jones's automobile to track his movements for over a month.[311] The court held that the warrantless GPS surveillance of a criminal suspect violates a suspect's reasonable expectation of privacy in her movements on a public thoroughfare.[312] This starkly contrasts with the position taken by other circuits, notably that taken by the Seventh Circuit in *Garcia*,[313] and the Ninth Circuit in *Pineda-Moreno*.[314] In *Garcia*, the court found that no search had occurred under the definition of the Fourth Amendment.[315] In reaching his conclusion, Judge Posner and the Seventh Circuit distinguished between technologies that merely improve the efficiency of otherwise legal law enforcement tactics and those that enable further intrusion.[316] Posner pointed to the use of thermal imaging in *Kyllo* as an example of technology that "reveal[ed] details of the interior of a home that could not otherwise be discovered without physical entry . . . ."[317] According to Posner, GPS tracking is merely a more efficient substitute for another perfectly legal activity—following a suspicious car.[318]

---

305. *See e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979); *Miller*, 425 U.S. at 443.
306. *Smith*, 422 U.S. at 744.
307. *Miller*, 425 U.S. at 442.
308. *Smith*, 425 U.S. at 744 (citing *Miller*, 425 U.S. at 442).
309. *Id*. at 745.
310. *See* Ashby Jones, *Should the Feds Have to Get a Warrant to Track Someone With GPS*? WALL ST. J. L. BLOG (Apr. 15, 2011, 6:24 PM), http://blogs.wsj.com/law/2011/04/15/should-the-feds-have-to-get-a-warrant-to-follow-someone-with-gps.
311. United States v. Maynard, 615 F.3d 544, 549 (D.C. Cir. 2010).
312. *Id.*
313. United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007).
314. United States v. Pineda–Moreno, 591 F.3d 1212, 1215 (9th Cir. 2010).
315. *Garcia*, 474 F.3d at 997.
316. *Id.* at 997–98.
317. *Id.* at 997 (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)).
318. *Id.*

On the contrary, the *Maynard* court used a fundamentally different rationale in reaching the opposite result. In finding that unwarranted GPS surveillance violates the Fourth Amendment, the D.C. Circuit focused on the *Katz* test in arguing that a person has a subjective expectation that her movements will not be recorded in an extended, uninterrupted manner.[319] Most interestingly, the court in *Maynard* noted that the marginal cost of every additional day of GPS surveillance was "effectively zero."[320] Based on this, the *Maynard* court found that the efficiency of GPS tracking in monitoring the whereabouts of a police suspect was previously unmatched, making it substantively more intrusive.[321] The court instead applied a "mosaic theory" in arguing that long-term surveillance of an individual reveals important and intimate details about their behaviors.[322] The Seventh Circuit's opinion in *Garcia* appears to be more consistent with the Supreme Court's previous holding. But the recent *Maynard* decision represents a new doctrinal current to categorize extraordinarily efficient technologies as uniquely intrusive, thus amounting to a search under the Fourth Amendment.

The *Maynard* holding may be seen as incongruent with previous judicial regulations of police investigations. Previous Fourth Amendment cases merely limit specific investigative techniques, like the use of an extrasensory technology, rather than limiting the overall breadth of an investigation. If the Court were to hold that the use of unwarranted GPS represents an investigative technique that is simply too intrusive because it aggregates discrete pieces of information, would the Court also limit the police from manually surveilling suspected criminals through more traditional means like stakeouts? And when would traditional, in-person surveillance of a criminal suspect reach such an intrusive degree as to require a warrant? The Supreme Court may be able to circumvent this doctrinal inconsistency by either condoning the warrantless use of GPS as a mere efficiency-enhancing technology tantamount to radio transmitters in *Knotts*, or by narrowly categorizing GPS devices as extrasensory in their capabilities to aggregate discrete data, thus requiring a warrant.

But regardless of how the Supreme Court holds in *Jones*, the digitally efficient investigative state is notably different from GPS surveillance in one important respect: networked community surveillance technologies like ALPR surveil an entire community as opposed to a specific individual. This suggests that even if the Court holds in *Jones* that the warrantless GPS surveillance of a single individual comports with the Fourth Amendment, the indiscriminate surveillance and data retention capabilities implicated by the digitally efficient investigative state nonetheless threaten basic constitutional protections.

319. United States v. Maynard, 615 F.3d 544, 563–64 (2010).
320. *Id*. at 565.
321. *Id*. at 565–66.
322. *Id*. at 562.

V. THE JUDICIAL RESPONSE TO THE DIGITALLY EFFICIENT INVESTIGATIVE STATE

Given the ominous implications of the digitally efficient investigative state, I argue that the courts should craft a judicial response that permits the use of surveillance technologies for some criminologically advantageous activities like observational comparison, but limits the unregulated data retention without reasonable suspicion. Further, I contend that the judiciary is well positioned to make this careful calculation, which admittedly requires the balancing of social values such as privacy and law enforcement efficiency. Overall, I conclude a judicial solution handed down by the courts would best safeguard citizenry, particularly certain discrete and insular minorities, from the threats posed by other emerging surveillance technologies.

A. The Judicial Response

The courts should craft a regulation that limits surveillance technologies in three ways. First, the courts should require police to have a legitimate, articulable law enforcement purpose before identifying any surveillance data. This would require police to identify a legitimate purpose for cross-referencing license plate data or facial recognition photographs with other government databases to ascertain the personal identity tied to the data. Second, the courts should require police departments to articulate and justify clear policies that limit the length of time police may retain surveillance data obtained through indiscriminate data collection practices without individualized, reasonable suspicion of criminal wrongdoing. Reasonable suspicion is a lower evidentiary standard than probable cause and merely requires law enforcement to demonstrate a particularized suspicion of criminal wrongdoing based on "specific and articulable facts" combined with "rational inferences."[323] Conversely, the courts should continue to permit the use of surveillance technologies for observational comparison, given that observational comparison only identifies an individual in surveillance data when the data has been digitally matched to a database of known or suspected criminals.[324] Hence, this recommended response would distinguish between mere observational comparison and the creation of indiscriminate "digital dossiers"[325] on personal movements. Third, the judiciary should carefully analyze the relationships between private data aggregators and law enforcement. A default rule permitting law enforcement to use any information obtained through voluntary information flows with private companies has understandable doctrinal appeal. Nonetheless, the courts should be vigilant in carefully determining whether a private party substantially collaborated and coordinated with law enforcement sufficient to transform that private party into a state actor.

This judicial response can be better understood when applied to ALPR.

323. Terry v. Ohio, 392 U.S. 1, 21 (1968).
324. *E.g.*, Sheridan, *supra* note 4, at C5.
325. *See* Solove, *supra* note 13, at 1084.

As discussed earlier, ALPR has two unique capabilities: an observational comparison capability and an indiscriminate data retention capability.[326] Police use the observational comparison capability to read passing license plates and then search for matches with active hotlists.[327] Once the ALPR system matches a license plate to a known offender, the ALPR system can cross-reference this plate with other databases to identify the suspected culprit. Observational comparison does not implicate any particular Fourth Amendment concerns—data is only retained and identified for cars matching a criminal database.[328] Conversely, the indiscriminate data collection capability allows some ALPR systems to record the license plate, time, and location of *every passing vehicle* into an expansive database.[329] This information can then be cross-referenced to other databases to identify the suspected driver of each car, and record that driver's movements into a surveillance database. It is not inconceivable that, with an extensive network of ALPR cameras in a given community, law enforcement could compile a fairly comprehensive record of an individual's day-to-day movements. Thus, by limiting the retention of data and requiring a legitimate law enforcement purpose before cross-referencing license plate numbers to identify drivers, this judicial response would prevent ALPR from transforming into a tool of mass surveillance.

In my view, this judicial regulation recognizes both the potential harms and benefits of the digitally efficient investigative state and strikes a fair balance. First, this proposed regulation ensures that the these technologies will not be utilized to unfairly target unpopular minorities—in fact, by distinguishing between observational comparison and indiscriminate data collection, the courts could ensure that these technologies are used primarily to reign in police discretion, thereby limiting implicit bias. As discussed *supra* in Part I.D.1, when limited to observational comparison, ALPR and facial recognition software can actually reduce the likelihood of racial or ethnic profiling. But as detailed *supra* in Part I.D.2, indiscriminate data collection capabilities of the digitally efficient investigative state can permit fishing expeditions and the targeting of politically unpopular minorities. By limiting the identification and retention of surveillance data, this regulation fights both profiling and the targeting of unpopular minorities.

Second, this proposed regulation is reasonably consistent with actual and recommended solutions proposed by legislatures, international courts, and domestic law enforcement organizations. Various legislatures have independently authored similar regulations on police technologies. The proposed judicial response bears some resemblance to legislative limits on surveillance technologies passed in Virginia, Maine, and New Hampshire. The New Hampshire law limits law enforcement surveillance to specific investigations of criminal wrongdoing and bars the retention of surveillance data except for a few, specific situations.[330] Maine, by contrast, has regulated

326. *See supra* Part II.A.1.
327. *E.g.*, Sheridan, *supra* note 4, at C5.
328. *Id*.
329. *Id*.
330. N.H. REV. STAT. §236:130 (2011).

ALPR technology explicitly by limiting data retention to 21 days and regulating ALPR usage more broadly.[331] This response also closely mirrors a recent German Federal Constitutional Court decision, which found that some parts of a German law authorizing the use of ALPR violated the right to privacy.[332] The German court held that the retention of any digital data that was not predestined for a specific use was too indiscriminate as to violate German Law.[333] The German court expressed concern that without limitations, the use of ALPR amounted to "complete surveillance."[334] Law enforcement organizations, namely the IACP, have also recommended that departments take steps, like transparent data retention policies, to ameliorate privacy concerns over surveillance data aggregation.[335]

Once more, this judicial response mirrors the principles laid out in the Organization for Economic Cooperation and Development (OECD) privacy guidelines.[336] Namely, this proposal requires that digital data collection on public movements abide by the OECD's purpose specification principle, which states that "the purposes for which personal data are collected should be specified not later than at the time of data collection."[337] Thus, there is both domestic and international precedent for this kind of judicial response to limit the efficiency of investigative technologies.

Third, the distinction between observational comparison and indiscriminate data aggregation comports with the underlying values of the Fourth Amendment. Regardless of the eventual holding in *Jones*, the *Maynard* decision offers persuasive application of the *Katz* doctrine to surveillance technologies.[338] The court first determined that the totality of a person's movements in public were not "actually exposed" to the public.[339] As the court explained, in determining whether "something is 'exposed' to the public[,] as that term was used in *Katz*[,] we ask not what another person can physically and may lawfully do, but rather what a reasonable person expects another might actually do."[340] Put differently, a person might reasonably expect a stranger to view any discrete action taken in public, but, "the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil."[341] In applying a "mosaic theory," the D.C. Circuit noted that that long-term surveillance of an individual reveals

---

331. ME. REV. STAT. 29-A, § 2117-A (2010).

332. Josh Ward, *The Hallmarks of a Totalitarian State*, SPIEGEL ONLINE INT'L (Mar. 12, 2008, 1:00 PM), http://www.spiegel.de/international/germany/0,1518,541025,00.html.

333. *See id*. (stating "that states would not be in violation of the Constitution if data were deleted. . . immediately after it was compared to databases").

334. *Id*.

335. *See* IACP PRIVACY ASSESSMENT *supra* note 25, at 37–42.

336. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORG. FOR ECON. CO-OPERATION & DEV., http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_ 1_1_ 1_1,00&&en-USS_01DBC.html (last visited Sept., 14, 2011).

337. *Id*.

338. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) (discussing warrantless use of GPS device on defendant's vehicle).

339. *Id*. at 558.

340. *Id*. at 559.

341. *Id*. at 560.

important and intimate details about their behaviors.[342] And because GPS surveillance is incredibly efficient—the marginal cost of each additional day of data aggregation with GPS tracking is "effectively zero"—GPS technology is thus a "heretofore unknown type of intrusion" requiring judicial regulation.[343]

The *Maynard* court's reasoning, while controversial in the context of the surveillance of a single individual, is extremely compelling when applied dragnet technologies like ALPR and surveillance cameras with facial recognition. As data collection costs decrease, law enforcement has every incentive to aggregate as much potentially useful data as possible. Indeed, as the *Maynard* court recognized, "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble."[344] Just as a person does not reasonably expect that the totality of her movements within an automobile to be monitored by GPS, she also reasonably expects to be free from continuous and pervasive monitoring by ALPR or facial recognition software. Even in public, we carry an expectation that our movements "remain 'disconnected and anonymous.'"[345] Hence, this recommended solution aligns with *Katz* by protecting a person's socially recognized, reasonable expectation to privacy, and follows the persuasive reasoning of the *Maynard* decision.

Fourth, the proposed limitation on data retention protects the criminological and evidentiary benefits of limited data retention, while also recognizing the retained data's loss of value over time. The recommended judicial response is admittedly vague—I do not specify an exact length of time the courts ought to permit law enforcement to retain data. This is omission is purposeful. As the IACP has properly recognized, any policy limiting data retention raises serious public policy concerns.[346] For example, we may prefer more liberal data retention policies for surveillance around national monuments and critical infrastructures in recognition of the threat posed by terrorism.[347] Further, there is a dearth of social science research on the changing usefulness of surveillance data over time. Nonetheless, without regulation departments have little incentive to self-regulate. While it may be difficult for the courts to craft a uniform national rule on data retention, the courts can at least require that departments, or conversely state legislatures, articulate clear data retention policies. This would permit states and localities to consider the unique criminological needs for data retention in their jurisdiction in crafting regulations, while preventing the indiscriminate collection of all data.

Admittedly, this suggested judicial response is a major doctrinal shift and requires the courts to break away from established Fourth Amendment doctrine. But the digitally efficient investigative state poses too many serious and constitutionally relevant threats for the judiciary to simply defer to

342. *Id*. at 562.
343. *Id*. at 565.
344. *Id*. at 562.
345. *Id*. at 563 (citing Nader v. Gen. Motors Corp., 255 N.E.2d 765 (N.Y. 1970)).
346. IACP PRIVACY ASSESSMENT, *supra* note 25, at 44.
347. *Id*.

legislative arrangements. Scholars have often argued that the legislature is better suited to assess the proper balance between privacy and security.[348] At least in the narrow field of police surveillance technologies, I disagree. In the next section, I argue that the courts are the best-positioned actor to address the issues implicated by mass data collection.

B. The Courts Are Better Positioned Than the Legislature to Regulate Police Technologies

The role of the judiciary in regulating technologies has been a point of contentious debate amongst legal scholars. Kerr has argued that judicial policymaking in the field of developing technologies "tend[s] to incorporate outdated assumptions of technological practice, leading to rules that make little sense in the present or future."[349] According to Kerr, the judiciary lacks the necessary resources to effectively regulate technology, making the legislature a more appropriate regulatory venue.[350] Several scholars, including Donald Dripps, have responded that legislatures are generally unwilling to create privacy-protective policies because "voters identify themselves as the potential victims of crime rather than its perpetrators."[351] According to Dripps, judicially crafted regulations governing police investigations are a legitimate and necessary protection of minority rights that does not usurp legislative prerogative.[352] I take this opportunity to weigh in on this debate by arguing that in the field of police surveillance technologies, the judiciary is the most institutionally competent actor to regulate police technologies and serve as a valuable counter-majoritarian force. While the so-called "judicial information deficit"[353] should deter the courts from micromanaging the use of law enforcement technology, it should not prevent the judiciary from implementing a reasonably tailored response to mass surveillance.

First, the courts are structurally well positioned within our decentralized federal system to address the national concern of mass surveillance. The courts are the most nonpartisan actor capable of protecting the rights of the disadvantaged and politically unpopular. If the courts defer to legislative arrangements, surveillance technologies will be regulated inconsistently across jurisdictions. The digitally efficient investigative state is no longer a localized phenomenon, but an increasingly national, centralized system. The judiciary is the most appropriate branch to develop a national solution that would be applicable to all law enforcement—local, state, and national. By grounding the judicial remedy in the Fourth Amendment, the judiciary can ensure that every person has a reasonably consistent expectation to privacy in the aggregation and sharing of personal data across jurisdictional lines.

---

348. *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 807 (2003–2004).

349. *Id*.

350. *Id*. at 807, 857–87.

351. *Id*. at 886 (discussing Dripps' theory); Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or, Why Don't Legislatures Give a Damn About the Rights of the Accused?* 44 SYRACUSE L. REV. 1079, 1088–90 (1993).

352. Dripps, *supra* note 351, at 1081.

353. Kerr, *supra* note 348, at 875.

Once more, legislative efforts to regulate surveillance may reify majoritarian preferences and insufficiently protect the privacy of certain politically unpopular minorities, like Muslim-Americans. There is a cogent argument to be made that, in the current heated and divisive political environment, Muslim-Americans are the individuals most at risk of indiscriminate surveillance data collection and subsequent fishing expeditions. Admittedly, Kerr points out that Congress has frequently "acted on its own initiative to protect privacy against the threat of new technology."[354] This descriptively suggests that Congress has been more receptive to the evolving privacy concerns than the courts. No doubt, Kerr is correct—courts have been predictably deferential and restrained in regulating law enforcement technologies. But this does not mean that the courts are not institutionally competent to create Fourth Amendment policy, particularly when data collection and surveillance raise delicate majoritarian concerns that cannot be adequately addressed by the legislature. Kerr rejects the majoritarian critiques of legislative arrangements by claiming that since "[p]rivacy and security may be considered public goods, shared equally by the public," and "both law enforcement interests and victims of crime may lobby the legislature," the judicial arrangements offer no substantial benefits over legislative arrangements.[355] Kerr also dismisses Dripps's majoritarian concern by noting that "new technologies will tend to target users of new technologies."[356] These users are disproportionately elite, meaning that their interests should be well represented in the legislature. Hence, Kerr believes that Dripps's concern that minorities will be underrepresented and marginalized in the political process is unwarranted. But Kerr's logic, while applicable in most situations, is unpersuasive in the current political environment. In the political hysteria surrounding the War on Terrorism, those most likely to be targeted by mass surveillance, indiscriminate data collection, and subsequent fishing expeditions may be politically unpopular minorities like Muslim-Americans. There is, undoubtedly, tremendous pressure on the Executive Branch and law enforcement to use any means legally available to prevent a terrorist attack on American soil. Anecdotal evidence suggests that law enforcement has targeted Muslim-Americans, in particular, for surveillance over the last decades. For example, a group of Muslim-Americans in California has accused the FBI of targeting religiously devout Muslim-Americans for surveillance, without any particularized suspicion of wrongdoing.[357] The American Civil Liberties Union (ACLU) has filed a class action complaint against the FBI in the Central District of California alleging that the FBI used an informant to "indiscriminately collect personal information on hundreds and perhaps thousands of innocent Muslim Americans in Southern California . . . . [T]he FBI did not gather the information based on suspicion of criminal activity,

354. *Id*. at 855.

355. *Id*. at 884–85.

356. *Id*. at 887.

357. *See, e.g.*, Patrik Jonsson, *Muslim Group Sues FBI over Surveillance at California Mosque*, CHRISTIAN SCI. MONITOR (Feb. 23, 2011), http://www.csmonitor.com/USA/Justice/2011/0223/Muslim-group-sues-FBI-over-surveillance-at-California-mosques. *See also* Jennifer Medina, *Suit Accuses F.B.I. of Spying at Mosques in California*, N.Y. TIMES, Feb. 25, 2011, at A17.

[but] instead it gathered the information simply because the targets were Muslim."[358]

Furthermore, it seems highly improbable that elites in the legislature will be responsive to the privacy concerns of these unpopular minority needs. Muslim-Americans, as an example, are also chronically underrepresented in the legislative branch.[359] Unpopular minorities are therefore unable to protect their right to be free from pervasive surveillance through legislative compromises. This represents a structural flaw in our decentralized federal system, one that can only be remedied by judicial action. The judiciary is the most institutionally competent actor to address the majoritarian concerns raised by mass surveillance and data collection.

Second, the so-called "judicial information deficit"[360] should not deter the courts from creating policy to address mass surveillance concerns. The proliferation and use of mass surveillance technologies has stabilized to a point that judicial action would be appropriate. In arguing that the judiciary lacks the skills and competence to create broad Fourth Amendment policy, skeptics have commonly levied three arguments: (1) unlike the legislature, the courts lack the physical and administrative resources to craft a comprehensive policy; (2) judges are not technologically sophisticated enough to create technology policy; and (3) once crafted, judicial technology policies rarely hold up in different factual scenarios.[361] As I demonstrate below, the limited judicial response offered in this Article will hold up against these three legitimate critiques.

To begin with, skeptics allege that legislations can more carefully analyze a problem, investigate potential solutions, impanel experts, and make far-reaching, nuanced policies.[362] Unlike the legislature, which may "command the resources of an extensive bureaucracy . . . a judge is generally limited to a secretary and one or two recent law school . . . [graduate clerks]."[363] Kerr has thus argued that the courts simply do not have the resources to engage in this kind of careful analysis necessary to develop a comprehensive and responsive policy on Fourth Amendment technologies.[364] On its face, this type of analysis is persuasive, especially considering the fact that the courts lack the funding to do sweeping investigations into the efficacy of an emerging technology. Nonetheless, this logic ignores a pivotal tactic used by courts in previous iterations of successful policymaking—the adoption of standards already implemented by other institutions.[365] Malcolm Feeley and Edward Rubin explained that when the courts attempted to create extensive judicial policy

358. Class Action Complaint at 1, Fazaga v. Fed. Bureau of Investigation, No. SACV11-00301 (C.D. Cal. Feb. 22, 2011).

359. *See Ellison to Swear on Jefferson's Qur'an*, MILWAUKEE J. SENTINEL, Jan. 4, 2007, at 6A (stating that Congressman Keith Ellison was the first and only Muslim American elected to Congress in U.S. history in 2006).

360. Kerr, *supra* note 348, at 875.

361. *Id*. at 875–77.

362. *Id*. at 881–82.

363. MALCOLM M. FEELEY AND EDWARD L. RUBIN, JUDICIAL POLICY MAKING AND THE MODERN STATE 307 (1998).

364. Kerr, *supra* note 348, at 858–59.

365. MALCOLM M. FEELEY & EDWARD L. RUBIN, *supra* note 363, at 307.

regulating American prisons, judges turned to the American Correctional Association and the Federal Bureau of Prisons.[366] Indeed, "[F]ederal judges turned to these standards because they wanted to impose detailed, administrative-style rules of any sort but lacked the resources to design the rules themselves."[367] Unlike the prison reform context described by Feeley and Rubin, where the courts created extensive and detailed policy, the judicial response I argue for in this Article does not require extensive investigation or uniform implementation. I merely argue for a judicially mandated floor, which establishes the minimum amount of regulation required for surveillance technologies. Additionally, there is domestic and international precedent, most notably in Maine, New Hampshire, Virginia, and Germany, that the courts could use as a model to craft a broad solution.[368] Once the courts lay out a broad policy objective, police departments and local legislatures would be incentivized to develop their own, individual policies to implement this judicially mandated, regulatory floor. States would be free to develop more complex, detailed, and even more stringent protections against data collection. Some states have already done just that.[369] This pattern can be seen in other areas of criminal judicial policymaking, such as *Miranda* requirements. The Court handed down broad general requirements—departments, in implementing the *Miranda* decision, often went above and beyond the Court's minimal requirements.

Next, critics of judicial regulation of emerging technologies have argued that judges are not as technically sophisticated as the legislature. Judges often "rely on the crutch of questionable metaphors to aid their comprehension" of complex technology cases, meaning that "it is easy for judges to misunderstand the context of their decisions and their likely effect when technology is in flux."[370] But in the unique situation outlined in this Article, judges do not need to be experts in these technological fields to understand the capabilities of technologies like ALPR and facial recognition software. The danger I discuss in this article is that police will keep a digital dossier of every single person's movements. This type of monitoring would facilitate fishing expeditions, increase the likelihood of corrupt behavior by law enforcement, and facilitate some types of racial profiling. There is little reason to believe that, with the assistance of knowledgeable advocates, judges could not sufficiently understand the potential harms posted by digitally efficient investigative technologies to develop a coherent constitutional floor of protection. And even though the legislature has a broader array of resources at its disposal, the legislature is an unsatisfactory avenue to protect the unique counter-majoritarian issues at stake.

Finally, some scholars have contended that judicial regulations of

366. *Id*.

367. *Id*.

368. *See supra* Part V.A. (describing judicial responses to legislative limits on police technologies).

369. *See* H.B. 454, 2002 Gen. Assemb., 2002 Sess. (Va. 2002) (implementing the restricted use of facial recognition technology in Virginia). *See also Facial Scan: Beach's Use Restricted Under Bill Approved by House*, THE VIRGINIAN-PILOT & LEDGER STAR, Feb. 13, 2002, at B4 (describing Virginia's facial recognition technology bill).

370. Kerr, *supra* note 348, at 875–76.

emerging technologies rarely hold up in different factual scenarios. Under this rationale, critics of this judicial response may contend that while this protection could work when applied to ALPR or facial recognition software, it would not necessarily be a workable standard for future technological developments. This view certainly has merit. "By the time the courts decide how a technology should be regulated . . . the factual record of the case may be outdated, reflecting older technology rather than more recent developments."[371] Stuart Benjamin has argued that "rapidly changing facts weaken the force of stare decisis by undermining the stability of precedents."[372] This provides a forceful case against judicial micromanagement of emerging technologies. But the judicial response argued for in this Article is sufficiently broad to avoid the predictable antiquation of other, narrower judicial solutions—it merely distinguishes between observational comparison and indiscriminate data collection, while broadly regulating the identification of data and interactions with private data aggregators. The collection of extensive, indiscriminate surveillance data is a widespread, pervasive occurrence common amongst countless investigative technologies. The development of digital dossiers is not a trending fad that will simply disappear in the near future. We should not expect the legislature to step in and address a problem that may disproportionately affect unpopular minorities. The Court has long recognized that when making policy in the field of emerging technologies, "the rule we adopt must take account of more sophisticated systems that are already in use or in development."[373] The judicial response presented does not prevent the use of surveillance technologies for observational comparison, but merely offers a sufficiently broad and generalized constitutional limit on indiscriminate data collection, which can be reasonably exported and applied to future, more sophisticated technologies.

Once more, critics of judicial policymaking seem tacitly concerned that the limited applicability of judicial rules in the future will weaken the force of stare decisis, thereby undermining the judiciary's legitimacy. But nothing could further de-legitimize the judiciary more than a failure to serve its fundamental role as a protector against the tyranny of majoritarian preferences. The courts are therefore the best-positioned actor within our decentralized federal system to protect against the threat of extensive, indiscriminate data collection. Concerns about the judiciary's institutional competence seem misplaced. And though the courts have limited resources, there is not enough convincing evidence of a "judicial information deficit"[374] so as to overcome the judiciary's important role as protectors of discrete and insular minorities.

C. Re-conceptualizing the Current Privacy Doctrine in Light of the Digitally Efficient Investigative State

A judicial response is a step in the right direction in addressing the

371. *Id*. at 869.

372. Stuart Minor Benjamin, *Stepping Into the Same River Twice: Rapidly Changing Facts and the Appellate Process*, 78 TEX. L. REV. 269, 272 (1999).

373. Kyllo v. United States, 533 U.S. 27, 36 (2001).

374. Kerr, *supra* note 348, at 875.

growing threat posed by mass police surveillance. But the proposed judicial response should only be the beginning in a broader shift in our privacy dialogue. The digitally efficient investigative state has wide-ranging social implications for the entire study of privacy law. I argue that, given the mounting evidence of efficient retention of public surveillance data and data centralization, it is finally time to re-conceptualize outdated privacy law assumptions—principal among them the antediluvian notion that an individual has no reasonable expectation to privacy in public movements. To be clear, I am not arguing that, descriptively, people *currently* have an honest expectation to privacy in public in today's world. In the age of GPS, smart phones, Facebook, and Twitter, our socially reasonable expectation to privacy is weaker than ever. Instead, it is time for a normative reassessment of our entire privacy doctrine. Of course, I am not the first to propose such an argument. Professor Solove has already observed:

> [P]rivacy is not simply an empirical and historical question that measures the collective sense in any given society of what is and has long been considered private. Without a normative component, a conception of privacy can only provide a status report on existing privacy norms rather than guide us toward shaping privacy law and policy in the future. If we focus simply on people's current expectation of privacy, our conception of privacy would continually shrink given the increasing surveillance in the modern world.[375]

The judiciary can and should play a fundamental role in protecting a normatively forceful conception of privacy in all regards. Do we reasonably expect a person to assume the risk that, every time they enter a public space, the state can monitor their every movement with ALPR? Do we reasonably expect a person to assume the risk that the state will keep extensive, centralized data on their movements indefinitely? Or perhaps the more important question is *should* we expect individuals to completely abandon all anonymity in public? I believe the clear, normative answer to these questions is a resounding *no*, and the implications of the digitally efficient investigative state only add weight to the claims previously made by Professor Solove and others.

Ultimately, this Article only scratches the surface of the broader social implications of the digitally efficient investigative state. Questions remain about the relative criminological benefits of observational comparison as compared to wholesale data retention. There is an increasing need for empirical research on the effects these emerging technologies have on individual behavior. And there is a dearth of concrete data on the extent to which law enforcement use these technologies. I offer only a brief glimpse into this new technological order, the relevant case law, and some general normative recommendations. This should only be the beginning of the conversation about the sociological, psychological, criminological, and legal impacts of the increasingly efficient police surveillance.

375. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1142 (2002).

VI. CONCLUSION

Neither judicial responses nor "legislative rulemaking is . . .a panacea."[376] Even if the judiciary successfully recognizes a remedy similar to that discussed in this Article, the legislatures must play a critical role in developing more nuanced and specific enactments to implement this constitutional floor. The potential harms of the digitally efficient investigative state are real. There is legitimate concern that the broad and integrated use of these technologies can create a mass surveillance state. Central to this debate is the proper role of the judiciary in regulating policy activity. Courts have previously relied upon an often fragile dichotomy between technologies that merely improve police efficiency and those that offer officers a new, extrasensory ability.

For the first time, the judiciary may be forced to limit the efficiency of law enforcement technologies. Implicit in this action will be the recognition that sometimes improvements in efficiency can be, quite simply, so efficient as to be unconstitutionally harmful. Unregulated efficiency can facilitate police wrongdoing, discrimination, and calumniate political dissenters. Unregulated efficiency in policing technology undermines central protections and tenants of a democratic state. The relationship between efficiency of criminal investigations and privacy rights will be a new frontier for the courts in the coming decades. The courts should forcefully, but prudently, protect against the unregulated efficiency of emerging investigative and surveillance technologies. The judicial response offered in this Article would be but one more example of the courts exercising their proper role as a limited but effective policymakers.

376. Kerr, *supra* note 348, at 881.