LOCAL LAW ENFORCEMENT JUMPS ON THE BIG DATA BANDWAGON: AUTOMATED LICENSE PLATE RECOGNITION SYSTEMS, INFORMATION PRIVACY, AND ACCESS TO GOVERNMENT INFORMATION

Bryce Clayton Newell

LOCAL LAW ENFORCEMENT JUMPS ON THE BIG DATA BANDWAGON: AUTOMATED LICENSE PLATE RECOGNITION SYSTEMS, INFORMATION PRIVACY, AND ACCESS TO GOVERNMENT INFORMATION

Bryce Clayton Newell[*]

I. INTRODUCTION

As government agencies and law enforcement departments increasingly adopt big-data surveillance technologies as part of their routine investigatory practice, personal information privacy concerns are becoming progressively more palpable. On the other hand, advancing technologies and data-mining potentially offer law enforcement greater ability to detect, investigate, and prosecute criminal activity. These concerns (for personal information privacy and the efficacy of law enforcement) are both very important in contemporary society. On one view, American privacy law has not kept up with advancing technological capabilities, and government agencies have arguably begun to overstep the acceptable boundaries of information access, violating the privacy of their citizens and decreasing the relevancy of the Fourth Amendment. On another, crime has decreased significantly over the past few decades,[1] thanks in part to more effective and efficient policing,[2] and criminal activity has become more technologically advanced as well; to unduly limit police would hamper legitimate efforts to keep our communities safe from serious crime.

Despite decades of increasingly safer streets and fewer instances of serious police-citizen violence in America,[3] the police continue to hold a highly criticized role in society.[4] Indeed, most recent press about police use of big data technologies

---

* Ph.D. Candidate, University of Washington (Seattle), Information School; M.S. in Information Science, University of Washington; J.D., University of California, Davis School of Law. The Author wishes to thank Adam D. Moore, Matt Fiske-Verkerk, Josef Eckert, Chris Heaney, and Katherine Thornton for their feedback and assistance with various aspects of this work. All remaining problems are those of the Author alone.

1. Although for a challenge to this general claim, arguing that the reality is a bit more complex. *See generally* ELLIOTT CURRIE, CRIME AND PUNISHMENT IN AMERICA (2013).

2. *See generally*, Brandon C. Welsh & David P. Farrington, *Surveillance for Crime Prevention in Public Space: Results and Policy Choices in Britain and America*, 3 CRIMINOLOGY & PUB. POL'Y 497 (2006) (providing evidence that visual CCTV surveillance and improved lighting in urban areas reduce certain types of crime).

3. *See* Daniel B. Wood, *US Crime Rate at Lowest Point in Decades. Why America Is Safer Now.*, CHRISTIAN SCI. MONITOR (Jan. 9, 2012), http://www.csmonitor.com/USA/Justice/2012/0109/US-crime-rate-at-lowest-point-in-decades.-Why-America-is-safer-now; David Seifman, *20 Years of Safer Streets*, N.Y. POST (May 11, 2013, 4:00 AM), http://nypost.com/2013/05/11/20-years-of-safer-streets; *see also Principles of Good Policing: Avoiding Violence Between Police and Citizens*, DEPT. OF JUSTICE, CMTY. REL. SERV., http://www.justice.gov/archive/crs/pubs/principlesofgoodpolicingfinal092003.pdf (last revised Sept. 2003)

4. For an earlier discussion of this phenomenon, see Egon Bittner, *The Functions of Police in Modern Society*, *in* ASPECTS OF POLICE WORK 89-102 (1990).

has focused on the negative implications that these developments have on citizen privacy—which is a very important concern[5]—but less attention has been given to balancing these privacy interests with the important societal interest in promoting effective and efficient police work. The tensions between these competing, equally legitimate aims is substantial and, in the context of police use of automated license plate recognition (ALPR) systems, limiting the scope of law enforcement data retention to protect citizen privacy (one option that has begun to find traction in Canada and in some U.S. states) might also protect the privacy of the police officers using these systems, as disclosure of these databases to the public under freedom of information (FOI) laws can allow citizens to track the historical policing patterns of individual officers.

Significant tensions exist between protecting citizen privacy and promoting open access to government surveillance information as a form of liberty-preserving citizen oversight; that is, if we protect privacy at all costs, we may risk limiting our democratic ability to oversee some government action and thus increase the potential for arbitrary government domination at direct cost to our freedom. Herein lies the second troubling conflict: limiting ALPR data retention not only protects the privacy of innocent individuals whose plates happen to be scanned, but it also limits the ability of the public to oversee police work, as a form of reciprocal surveillance, because the records available under FOI laws would be much more limited. Thus, the interests behind FOI laws, including the implicated First Amendment rights to gather information about government conduct, and personal privacy rights are in direct tension, in addition to the more obvious conflict between privacy and security.

As mentioned above, despite the obvious threats to personal information privacy posed by the increased adoption and use of sophisticated ALPR technologies by law enforcement, FOI laws in some jurisdictions have also been allowing citizens to access information about policing patterns and the historical movement patterns of law enforcement officers utilizing ALPR systems. In essence, these government agencies have been releasing their ALPR databases, including un-redacted license plate numbers, to members of the public through public disclosure requests. These databases may contain not only the license plate information of each vehicle scanned by the system, but also identifying information about the patrol vehicle that facilitated the scan, including precise date, time, and geo-location information of each scan, allowing citizens to track the patrol patterns of police vehicles outfitted with ALPR cameras. Thus, in a very real sense, the surveillance technologies used by the government have become a tool for citizen-counter-surveillance and a mechanism for oversight.

It should also be noted that this type of willing disclosure by law enforcement

---

5. For other work in this vein by the same author, see Bryce Clayton Newell, *The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe*, 9 I/S: J. L. & POL'Y INFO. SOC'Y. (forthcoming 2014), *manuscript available at* http://ssrn.com/abstract=2339338; Bryce Clayton Newell & Joseph T. Tennis, *Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs*, *in* ICONFERENCE 2014 PROCEEDINGS 345-55 (2014), *available at* https://www.ideals.illinois.edu/bitstream/handle/2142/47299/109_ready.pdf?sequence=2; Bryce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, 17 RICH. J.L. & TECH. 12, 32 (2011).

indicates either 1) a strong commitment to a high level of departmental transparency, which ought to be applauded; and/or 2) simply an absence (for whatever reason) of any relevant state public records exception that might be used to deny these disclosure requests. In Minneapolis, Minnesota, the public disclosure in 2012 of an ALPR database and the subsequent publication of the location of all 41 scans of the Mayor's license plate contained in the data[6] resulted in a temporary data classification that exempts ALPR data from public disclosure in that state until August 1, 2015 or until the Minnesota Legislature acts on the issue, whichever occurs first.[7] The American Civil Liberties Union applauded the temporary classification.[8] But, in some significant ways, this classification alone, without other measures to ensure public oversight of the ALPR system's use, is unfortunate and should not necessarily be endorsed.

In Seattle, Washington, the situation has not taken this same unfortunate turn, at least at present, although the Seattle situation presents its own problems. The Seattle Police Department (SPD) has been releasing ALPR databases to the public for some time and, based on prior events involving conflicts in Seattle between privacy and public disclosure, there are at least two reasons[9] to suggest that the SPD's continuing disclosures are motivated by an interest in transparency. However, the SPD practices are not without their own faults and, incidentally, such faults are generally shared by most other police departments around the country.

Part II of this paper explores some of the privacy-related ramifications of publicly accessible geo-spatial databases by relying on some recent controversies surrounding the publication of publicly accessible geo-spatial data. In Part III, the paper analyzes recent social and legal developments in the United States related to ALPR use by local law enforcement. The recent Canadian experience in British Columbia, which resulted in the provincial Information and Privacy Commissioner demanding changes to data retention and information-sharing practices of the Victoria Police Department (VPD) and the Royal Canadian Mounted Police (RCMP) provides some interesting comparative points of reference. Part IV presents an overview of Fourth Amendment privacy and the concept of privacy in public and questions the proper role of ALPR systems in police practice against the requirements of the Fourth Amendment to the United States' Constitution.

Part V consists of initial findings from an exploratory empirical analysis of

---

6. *See* Catherine Crump, *You Are Being Tracked: How License Plate Readers are Being Used to Record Americans' Movements*, ACLU, July 2013, at 3, *available at* https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf; Eric Roper, *City Cameras Track Anyone, Even Minneapolis Mayor Rybak*, MINNEAPOLIS STAR TRIB., (Aug. 17, 2012), http://www.startribune.com/local/minneapolis/166494646.html; Eric Roper, *Police Cameras Quietly Capture License Plates, Collect Data*, MINNEAPOLIS STAR TRIB. (Aug. 10, 2012), http://www.startribune.com/local/minneapolis/165680946.html.

7. *See generally*, Crump, *supra* note 6; *Current Temporary Classifications*, MINN. DEP'T OF ADMIN., INFO. & ANALYSIS DIV., http://www.ipad.state.mn.us/docs/tccurrent.html (last visited Jan. 18, 2014).

8. *See generally* Crump, *supra* note 6.

9. These include 1) prior use of state privacy law to defend withholding dash-camera footage under state public disclosure law to protect bystander privacy (without any similar attempt in the case of ALPR data), and 2) a renewed SPD 20/20 transparency program. *See SPD 20/20 – A Vision for the Future*, SEATTLE.GOV, http://www.seattle.gov/spd2020 (last visited Jan. 18, 2014).

two databases of ALPR data received under state FOI law from the SPD amounting to approximately over 1.7 million ALPR scans[10] over a roughly three-month period (the "SPD Databases"). In Part VI, the paper examines the efficacy of FOI laws that provide public access to these databases that contain a great deal of personally identifiable information, and the proper role of public access in establishing a form of reciprocal surveillance intended to promote responsible citizen oversight and preserve individual freedom.

Finally, in conclusion, the paper provides a normative argument for the right of privacy in personal information in public spaces, balanced against the important societal interest in government transparency and open access to government information. This normative theory attempts to account for and differentiate between the different roles of citizens and public officials carrying out their official duties, and their respective rights to privacy in public spaces. This normative argument provides a prescription for ALPR data privacy practices while still ensuring a certain level of public access to government information.

II. PUBLIC OUTRAGE OVER PUBLIC ACCESS

A number of recent developments highlight the building tensions between FOI or access to information (ATI) laws and the personal privacy interests of individual members of the public. As government agencies increasingly collect, use, sell, share, and archive personal information for various purposes (whether to protect national security interests, facilitate more efficient policing, or administer government programs), the informational privacy rights of individuals are potentially threatened when this personal information is publicly accessible under local or national FOI or ATI laws. This apparent tension pits two ideals directly against each other. Open access to government information serves as an important check on government power and abuse; one used by journalists and others for very legitimate reasons. Privacy rights in personal information also provide some check on government overreaching, as demonstrated by the Fourth Amendment's prohibition on unreasonable search and seizure and by the line of decisional privacy decisions handed down by the United States Supreme Court following *Griswold v. Connecticut*.[11] In some instances, these tensions have been highlighted by the online mapping of publicly accessible geo-spatial information, and these developments have spurred both legal change and public outrage.

A. The New York Gun Map

In response to the tragic shootings at Sandy Hook Elementary in Newtown, Connecticut in December 2012, a suburban New York state newspaper filed public records requests for the personal information of all pistol permit holders within three nearby counties. Subsequently, the paper generated and published an interactive online map that included the names and addresses of each of the

10. The data includes data from two separate databases, each connected to a different ALPR system in use by the SPD during the relevant timeframe. The two databases contain a total of 1,779,266 rows of license plate scans (at one row per scan) (not excluding certain rows generated by the systems for other purposes).

11. 381 U.S. 479 (1965).

individuals who had pistol permits in two of these counties (Rockland and Westchester).[12] The newspaper received the gun permit information through public records requests, and the data was released as publicly accessible information under state FOI law. Needless to say, the map—sourced from publicly available information—caused quite a controversy. In response, the New York legislature quickly passed the New York Secure Ammunition and Firearms Enforcement Act ("NY SAFE Act"), which amended the state Penal Law to allow gun owners to request that their permit applications become exempt from public disclosure.[13]

Following the enactment of the NY SAFE Act, the newspaper took its map offline.[14] The amended state Penal Law also had some slightly counter-intuitive ramifications. Prior to enactment, pistol permit holders' personal information had been shielded from disclosure to commercial entities seeking to use the information for marketing purposes, but not to the broader public. After the NY SAFE Act came into force, however, this personal information was no longer shielded unless the individual permit holders file the appropriate form seeking an exemption.[15] Thus, marketing companies now gain greater access to this personal information, unless individual gun owners take affirmative steps to protect their privacy.

B. Proposition 8 Donor Map

While information about donations to political campaigns or ballot initiatives can serve a valuable purpose, releasing this information publicly may also lead to harassment and disincentivize political donations from citizens who are concerned about being publicly associated with a sensitive political position. This scenario was played out clearly when personal information of donors to the campaign for California's Proposition 8 in 2008, which would have prohibited same-sex marriages in California, was overlaid onto Google Maps, thus allowing a visual, map-based, searchable database of Proposition 8 supporters.[16] As a consequence, supporters were targeted by death threats, scare tactics, and boycotts of supporter-owned businesses.[17] California access law made names, zip codes, employer information, and donation amounts public. While exact addresses and contact information were not included in the released data, this information could easily be determined using simple web-based services.

---

12. *See, e.g.*, Julie Moos, *Newspaper Publishes Names, Addresses of Gun Owners*, POYNTER.ORG, http://www.poynter.org/latest-news/mediawire/199148/newspaper-publishes-names-addresses-of-gun-owners (last updated Jan. 7, 2013).

13. *See Public Records Exemption - FOIL Form FAQ*, N.Y. DIV. OF ST. POLICE, http://www.troopers.ny.gov/Firearms/Public_Records_Exemption (last visited Jan 18, 2014).

14. *See* Andrew Khouri, *N.Y. Newspaper Removes Online Map of Gun-permit Holders*, L.A. TIMES, Jan. 20, 2013, http://articles.latimes.com/2013/jan/20/nation/la-na-nn-new-york-newspaper-gun-permits-map-offline-20130119.

15. *See* Glenn Coin, *NY Safe Act Requires Onondaga County to Release Many Pistol Permit Holders' Names, State Official Says*, SYRACUSE.COM (Aug. 13, 2013), http://www.syracuse.com/news/index.ssf/2013/08/onondaga_county_must_release_pistol_permit_holders_names_addresses_says_state_op.html.

16. *See* Brad Stone, *Prop 8 Donor Web Site Shows Disclosure Law is 2-Edged Sword*, N.Y. TIMES, Feb. 8, 2009, at BU3, *available at* http://www.nytimes.com/2009/02/08/business/08stream.html.

17. *Id.*

III. ALPR USE IN THE UNITED STATES, CANADA, AND THE UK

As the world now knows, the National Security Administration (NSA) has been collecting vast amounts of personal information about American citizens (in some cases breaking its own rules and violating the Constitution) and has been sharing this information, sometimes even in raw, un-redacted form, with friendly foreign intelligence agencies.[18] Closer to home, many local governments have been quietly amassing large databases of scanned license plates through the use of automated license plate recognition (ALPR) systems that can scan and track the movements of vehicles within their jurisdictions (and beyond, through inter-departmental collaboration and the aggregation of local databases).[19] In fact, according to one recent survey with responses from over 70 agencies, 85% of responding police departments had or expected to implement ALPR technologies within the next five years, and 70 percent of responding agencies reported that they already used some form of predictive policing, defined as "the advanced use of information/technology to predict and prevent crime."[20] Importantly, as indicated earlier, not all use of these systems is inappropriate or even unwanted, but the competing tensions between individual privacy, an effective and efficient criminal justice system, and public disclosure of government information makes the topic ripe for informed and thoughtful analysis.

In the United States, ALPR systems have become popular with local law enforcement and various state and local transportation departments. Government agencies are using these systems to track commercial carriers, facilitate quicker passage on toll roads and bridges, and to detect traffic congestion and estimate travel times to help motorists navigate away from congested streets or freeways. Police departments are also using these systems, whether mounted on stationary poles, parking enforcement vehicles, or patrol cars, to locate stolen vehicles or other vehicles of interest, and to detect vehicles with unpaid parking tickets as a way to generate additional revenue.

In 2012, the American Civil Liberties Union filed 587 freedom of information requests with local law enforcement and other state agencies around the country seeking information about ALPR use, resulting in over 26,000 pages of released documentation after just 293 responses (50% of the total requests).[21] These responses indicate that, as a general observation, less than 1 percent of scans actually result in a "hit"—or a scan of a license plate in a police database because of some (at least alleged) connection to on-going or previous infraction or

---

18. *See* Glenn Greenwald, Laura Poitras & Ewen MacAskill, *NSA Shares Raw Intelligence Including Americans' Data with Israel*, THE GUARDIAN (Sept. 11, 2013), http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents; Newell, *supra* note 5.

19. *See, e.g.*, Ryan Gallagher, *Police Across U.S. Quietly Turning to Cameras That Track All Vehicles' Movements: Survey*, SLATE.COM (Jan. 14, 2013, 4:27 PM), http://www.slate.com/blogs/future_tense/2013/01/14/automatic_license_plate_readers_survey_shows_most_u_s_police_agencies_plan.html.

20. *See* POLICE EXEC. RESEARCH FORUM, CRITICAL ISSUES IN POLICING SERIES: HOW ARE INNOVATIONS IN TECHNOLOGY TRANSFORMING POLICING? 1 (Jan. 2012), *available at* http://policeforum.org/library/critical-issues-in-policing-series/Technology_web2.pdf.

21. *See* Crump, *supra* note 6, at 3.

suspicious or criminal activity.[22]

Surveillance in public spaces is becoming increasingly common,[23] and in our modern society, corporations, organizations, governments, and even other individual citizens are the surveillance agents.[24] In the United States, our presence in a public space has generally equated to a waiver of any legally enforceable right to privacy for anything we do or say in those places—or in information about our physical location—on the premise that such information has been voluntarily disclosed to third parties by virtue of our very presence in public itself.[25] In the following sections, this paper survey's the legal landscape, explores the contents of an actual ALPR database, and questions whether rapidly advancing surveillance technologies (and particularly ALPR, for present purposes) should cause us to rethink how we approach regulating law enforcement collection and retention of ALPR data, protecting (or not protecting) privacy in public, and access to government information.

A. The Law in the United States

At present in the U.S., only six states have laws on the books that directly regulate the use of ALPR systems by law enforcement[26] and at least two others have regulated ALPR use by a directive from the state Attorney General's office.[27] At least three other states and federal authorities are also considering ways to regulate such systems,[28] additional states have toll collection or traffic stop statutes

---

22. *Id.* at 13.

23. *See generally* Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281 (2011); ADAM D. MOORE, PRIVACY RIGHTS: MORAL AND LEGAL FOUNDATIONS 1 (2010) ("Beyond data mining, video surveillance, facial recognition technology, spyware, and a host of other invasive tools are opening up private life for public consumption.").

24. Gary T. Marx, *Surveillance and Society*, *in* ENCYCLOPEDIA OF SOCIAL THEORY 817-22 (G. Ritzer ed., 2005), *available at* http://web.mit.edu/gtmarx/www/surandsoc.html.

25. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); Helen Nissembaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHIL. 559, 567 (1998); Helen Nissembaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7 ETHICS & BEHAV. 207, 212 (1998). *But see* Von Hannover v. Germany, 2004-III Eur. Ct. H.R. 294 (opposing view from the European Court of Human Rights); Newell, *supra* note 5, at 32.

26. *See* Crump, *supra* note 6, at 31 (noting five states with ALPR laws and two with state Attorney General opinions).

27. *See* Va. Op. Att'y Gen., Opinion No. 12-073, 2013 WL 653025 (Feb. 13, 2013); Directive No. 2010-5: Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data from Paula T. Dow, Att'y Gen., N.J., to Dir., Office of Homeland Sec. & Preparedness, et al., (Dec. 3, 2010), *available at* http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf [hereinafter Directive No. 2010-5].

28. *See, e.g.*, S.B. 226, 2014 Sess. (Fla. 2014), *available at* http://www.flsenate.gov Session/Bill/2014/0226/BillText/c2/PDF (exempting ALPR data from public disclosure); H.B. 3068, 188th Sess. (Mass. 2013), *available at* https://malegislature.gov/Bills/188/House/H3068; Press Release, State Rep. Sam Singh, State Rep. Sam Singh Announces Bill to Regulate Use of License Plate Readers (Sept. 4, 2013), *available at* http://069.housedems.com/news/article/state-rep-sam-singh-announces-bill-to-regulate-use-of-license-plate-readers.

that refer to ALPR,[29] and some states have case law precedent related to the use of ALPR for various purposes, including traffic stops.[30] In the five states with enacted legislation, regulation is not at all consistent.

1. New Hampshire

In New Hampshire, the state's Highway Surveillance law strictly prohibits the use of ALPR systems,[31] as well as other forms of technologically-aided means of "determining the ownership of a motor vehicle or the identity of a motor vehicle's occupants on the public ways of the state or its political subdivisions" by state or local government agents.[32] This prohibition extends to the use of "any" device, including cameras or other imaging devices, a "transponder, cellular telephone, global positioning satellite, or radio frequency identification device," when used to determine the ownership of the vehicle or identity of a person inside the vehicle.[33]

The law does provide for a number of exceptions, however, and new exceptions became effective in the latter half of 2013. These exceptions allow state agents to conduct such surveillance to facilitate operation of toll collection systems,[34] to provide security for three named bridges in Portsmouth,[35] when such surveillance is incidental to state monitoring of state-controlled buildings,[36] is undertaken "on a case-by-case basis" to investigate specific crimes,[37] or when images and data are viewed in connection with a specific incident on a public roadway (but recording is not allowed).[38]

Importantly, the law also prohibits the state and its political subdivisions from obtaining any information—specifically, ALPR and related data—that it could not collect on its own, regardless of whether the information is from private corporations or other federal or state entities.[39] This clause limits the ability of law enforcement agencies within New Hampshire to access national license plate scan databases or to receive license plate information from agencies in other states, unless the information-sharing was undertaken in order to investigate a specific crime (or under another exception as noted above).

2. Maine

Maine's Motor Vehicle Code prohibits private use of ALPR technology and

---

29. *See* ARIZ. REV. STAT. § 28-7751(3), (16) (West, Westlaw through 2013 legislation) (toll collection); MD. CODE ANN. TRANSP. § 25-113(a)(6)(ii)(4) (West, Westlaw through 2013 legislation) (traffic stops).

30. *See* Hernandez-Lopez v. State, 738 S.E.2d 116 (Ga. Ct. App. 2013); People v. Davila, 901 N.Y.S.2d 787 (N.Y. Sup. Ct. 2010).

31. *See* N.H. REV. STAT. ANN. § 261:75-b (2007) (prohibiting "automated number plate scanning devices").

32. *Id.* § 236:130(I) (2013).

33. *Id.*

34. *Id.* § 236:130(III)(e).

35. *Id.* § 236:130(III)(f).

36. *Id.* § 236:130(III)(d).

37. *Id.* § 236:130(III)(b).

38. *Id.* § 236:130(III)(c).

39. N.H. REV. STAT. ANN. § 236:131 (2006).

places restrictions on government use of such systems.[40] Interestingly, Maine's statute covers a much more limited set of technologies than the New Hampshire law, defining ALPRs more narrowly. Another section of the code, however, also restricts the ability of government agencies from enforcing traffic violations through the use of red-light or other traffic surveillance cameras.[41] Under the Maine law, ALPR is defined as a "system of one or more mobile or fixed high-speed cameras combined with computer algorithms to convert images of registration plates into computer-readable data."[42] Exceptions allow law enforcement and the Maine Turnpike Authority to use ALPR for toll enforcement.[43] The statute also allows the Maine Department of Transportation, the Department of Public Safety's Bureau of State Police, and other state and local law enforcement agencies to utilize ALPR for certain stated purposes.[44]

To alleviate privacy concerns, the statute restricts the ability of law enforcement officers to enter data into the system that does not relate to an ongoing investigation or that is not based on articulable facts suggesting safety concerns or criminal wrongdoing,[45] and any non-hit data (or data not retained by the Bureau of State Police for motor vehicle screening purposes) must be purged from the database within 21 days from initial capture.[46] The statute also specifically exempts ALPR data from public disclosure under the state FOI law,[47] which obviously protects the privacy of individual drivers and vehicle owners but limits the availability of data that could be used as a tool of public oversight.

3. Arkansas

In 2013, the Arkansas General Assembly enacted House Bill 1996, the Automatic License Plate Reader System Act, to regulate the use of ALPR systems within the state.[48] The Arkansas law also prohibits ALPR use, both by private and public entities,[49] and provides a number of exceptions where such use is permitted for certain purposes.[50] It also limits the use of ALPR data as evidence in court when the act is violated, and provides for a private cause of action,[51] including a clause allowing costs and the greater of actual damages or $1,000 per violation, for violations of the ALPR limitations.[52] Private use is only permitted when such systems are used to control access to secured areas not accessible to the public[53] or to regulate the use of parking facilities.[54] However, government parking and law

40. *See* 29-A M.R.S.A. § 2117-A (2010 & Supp. 2013).
41. *See id.* § 2117.
42. *Id.* § 2117-A.
43. *Id.* § 2117-A(1).
44. *Id.* § 2117-A(3).
45. *See id.*
46. *See id.* § 2117-A(5).
47. *Id.* § 2117-A(4).
48. *See* ARK. CODE ANN. § 12-12-1801-1808 (West, Westlaw through 2013 legislation).
49. *See id.* § 12-12-1803(a).
50. *See id.* § 12-12-1803(b).
51. *See id.* § 12-12-1807(a).
52. *Id.* § 12-12-1807(b).
53. *See id.* § 12-12-1803(b)(3).
54. *Id.* § 12-12-1803(b)(a)-(b).

enforcement agencies can also use ALPR systems to regulate the use of parking facilities or to compare captured plate data against hot listed plate information from certain specified sources, respectively.[55]

The Arkansas law also provides some thoughtful regulation of the retention and sharing of captured plate data. Generally, ALPR data captured may not be shared, sold, or disclosed to other entities,[56] except that law enforcement may share captured plate data with other law enforcement agencies as long as the scan data is evidence of an offense.[57] Otherwise, captured plate data may not be used for purposes other than those discussed above. Non-hit data must also be deleted within 150 days of initial capture[58] and, to help ensure compliance, the law also requires law enforcement to update their databases every 24 hours.[59] However, data collected by law enforcement that is related to an on-going investigation may be retained until the conclusion of criminal proceedings.[60]

The Arkansas Act does generally exclude public access to actual ALPR scan data, and restricts disclosure only to, or with the consent of, the person to whom the vehicle is registered.[61] The law also requires entities using ALPR systems to promulgate official policies,[62] and to compile and retain regular statistical reports to provide the public with information about the use and efficacy of the technology.[63] In particular, the law requires disclosure of the total number of scans, the number of scans resulting in arrest and prosecution, the names of the hot list categories that plate data was compared against, the number of confirmed hits or matches with information in the hot listed categories, and the total number of false positives (e.g., matches improperly made due to faulty character interpretation by an ALPR system's character recognition software).[64]

4. Utah

Utah also passed ALPR legislation in 2013, with the enactment of the Automatic License Plate Reader System Act,[65] which regulates the use of such systems and also amended the state public records law to exclude public access to ALPR data[66] (with certain exceptions under the state protected records provisions[67] or via certain court orders or a judicial warrant).[68] The Utah law also defines ALPRs narrowly, with almost identical language as that used in the Maine and

55. *See id.*
56. *See id.* § 12-12-1804(d)(1).
57. *Id.* § 12-12-1804(d)(2).
58. *Id.* § 12-12-1804(a).
59. *Id.* § 12-12-1804(c).
60. *See id.* § 12-12-1804(b).
61. *See id.* § 12-12-1808(a)(1); *see also id.* § 12-12-1805(b)(4).
62. *Id.* § 12-12-1805(b)(4).
63. *See id.* § 12-12-1805(a).
64. *See id.* § 12-12-1805(b)(1)-(3); *see also id.* § 12-12-1808(a)(2).
65. S.B. 196, 2013 Gen. Sess. (Utah 2013), *available at* http://le.utah.gov/~2013/bills/sbillenr/SB0196.htm.
66. *See* UTAH CODE ANN. § 63G-2-305(65) (West, Westlaw current through 2013 legislation); *id*. § 41-6a-2004(1).
67. *See id.* § 63G-2-202(4); *see also id*. §§ 63G-2-2002(4)-(7).
68. *See id*. § 41-6a-2004(1)(d).

Arkansas laws,[69] and other sections of the law track the language used in the Arkansas law as well. The Act allows broader exceptions than the Arkansas law, however. In addition to allowing law enforcement to compare ALPR scan data with hot list databases, the Utah law also allows police to use ALPR systems "for the purpose of protecting public safety, conducting criminal investigations, or ensuring compliance with local, state, and federal laws."[70] The Utah law also allows ALPR use for enforcing parking regulations, to regulate use of parking facilities, controlling access to secure areas, for collecting electronic tolls, and for "enforcing motor carrier laws."[71]

Private entities may not store ALPR data for longer than 30 days and public agencies must delete data within nine months, unless the data is subject to a preservation request, disclosure order, or properly issued warrant.[72] The law also prohibits selling or sharing ALPR data for reasons not enumerated in the statute, and allows—but does not require—ALPR users to compile aggregated reports or compilations of ALPR data and to conduct statistical analysis of the captured data, as long as the records are anonymized.[73] Finally, the law contains provisions for preservation orders requiring agencies to preserve captured data under certain circumstances.[74]

5. Vermont

Vermont's ALPR law was also enacted in 2013.[75] It defines an ALPR system just as in Maine, Arkansas, and Utah, but differentiates between "active" and "historical" data.[76] Active data includes plate information entered into system hot lists and plate data captured by routine use of ALPR systems, whereas historical data is defined as any ALPR data "stored on the statewide ALPR server operated by the Vermont Justice Information Sharing System of the Department of Public Safety."[77] Thus, Vermont has legislatively authorized a statewide ALPR database that facilitates information sharing between state and local agencies. As evidenced by an ALPR End User Agreement obtained by the American Civil Liberties Union of Vermont in 2012, the State stored plate information for four years[78] prior to enactment of the ALPR law, which limited retention to 18 months in most cases.[79] This database is the primary repository for ALPR data collected within the state, as the law requires law enforcement agencies using ALPR systems to upload their

69. *See id.* § 41-6a-2002(1) (defining an "[a]utomatic license plate reader system" as "a system of one or more mobile or fixed automated high-speed cameras used in combination with computer algorithms to convert an image of a license plate into computer-readable data.").

70. *Id*. § 41-6a-2003(2)(a).

71. *Id.* §§ 41-6a-2003(2)(a)-(f).

72. *Id*. § 41-6a-2004(c).

73. *Id*. §§ 41-6a-2004(2)(a)-(c).

74. *Id*. § 41-6a-2005.

75. VT. STAT. ANN. tit. 23, § 1607 (West, Westlaw current through 2013 legislation).

76. *Id.* at § 1607(a).

77. *Id*. §§ 1607(a)(1), (3).

78. Vt. Dept. of Pub. Safety, Div. of Crim. Just., ALPR End User Agreement, *available at* http://www.acluvt.org/legal/docket/files/alpr/dept_of_pub_safety_docs/Vt.%20Dep't%20of%20Pub.%20Safety%20ALPR%20data%20agreement.pdf (last visited Jan. 30, 2014).

79. *See* VT. STAT. ANN. tit. 23, § 1607(d)(2).

scan data to the statewide server.[80] The Vermont law allows the Vermont Information and Analysis Center, which manages the database, to share historical ALPR data with both Vermont and out-of-state law enforcement agencies for certain law enforcement purposes.[81]

The statute also requires officers to be certified to operate an ALPR system,[82] and restricts use of ALPR systems to certain enumerated "legitimate law enforcement purposes."[83] Officers are also prohibited from accessing active ALPR data or inputting plate information for non-legitimate purposes.[84] The law requires written requests to review data and limits access to ALPR information collected more than seven days prior to the request.[85]

For oversight purposes, the law requires the Department of Public Safety to institute internal safeguards to ensure that law enforcement are using the systems in accordance with the law, and also requires the Department submit an annual report to the State legislature detailing the number of ALPR units in operation statewide, the number of units transmitting data to the state servers, the total numbers of scans submitted by each agency to the state servers, the total number of scans contained in the 18-month state-run repository, the total number of requests for ALPR data from the state database, and the number of these requests fulfilled (for domestic and out-of-state requestors).

6. California

California's Vehicle Code authorizes the California Highway Patrol (CHP) to utilize ALPR data but limits retention to 60 days, unless the "data is being used as evidence" in a felony case.[86] The Code mandates internal monitoring for unauthorized use of ALPR data[87] and also specifies that the CHP

> shall not sell LPR data for any purpose and shall not make the data available to an agency that is not a law enforcement agency or an individual who is not a law enforcement officer. The data may be used by a law enforcement agency only for purposes of locating vehicles or persons when either are reasonably suspected of being involved in the commission of a public offense.[88]

The CHP must also submit information about ALPR usage (including data disclosures) to the state legislature as part of its annual vehicle theft report.[89] In addition to CHP usage, many other jurisdictions in California maintain ALPR systems, and the Northern California Regional Intelligence Center (NCRIC)

---

80. *See id.* § 1607(d).

81. *See id.* § 1607(c)(2)(A).

82. *Id.* § 1607(a)(4).

83. *Id.* § 1607(a)(5) ("'Legitimate law enforcement purpose' applies to access to active or historical data and means investigation, detection, analysis, or enforcement of a crime, traffic violation, or parking violation or operation of AMBER alerts or missing or endangered person searches.").

84. *Id.* § 1607(c)(1)(B).

85. *Id.* § 1607(c)(1)(C).

86. CAL. VEH. CODE § 2413(b) (West, Westlaw current through 2013 legislation).

87. *Id.* § 2413(d).

88. *Id.* § 2413(c).

89. *Id.* § 2413(e).

coordinates ALPR data from over 20 police departments.[90]

7. Virginia

In Virginia, the state Attorney General has issued an opinion limiting state law enforcement from collecting passive ALPR data (i.e., passively scanning and storing every plate passing by) under the Government Data Collection and Dissemination Practices Act.[91] Instead, law enforcement can only use license plate readers to "actively" scan and store plates that have been particularly identified, "evaluated and determined to be relevant to criminal activity."[92]

8. New Jersey

In New Jersey, law enforcement use of ALPR systems is regulated by an Attorney General Directive promulgated in 2010.[93] The Directive itself explicitly recognizes the role of mining ALPR data for detecting suspicious patterns—a form of predictive policing.[94] It also provides guidelines[95] for ALPR use by state and local law enforcement agencies, and requires them to develop policies consistent with these guidelines. These guidelines attempt to ensure that plate numbers are only entered into ALPR hotlist databases for legitimate law enforcement purposes, that ALPR data is only accessible by appropriate personnel, and to ensure data is "purged after a reasonable period of time."[96] Additionally, the guidelines state that law enforcement policies should be designed

> to permit a thorough analysis of stored ALPR data to detect crime and protect the homeland from terrorist attack while safeguarding the personal privacy rights of motorists by ensuring that the analysis of stored ALPR data is not used as a means to disclose personal identifying information about an individual unless there is a legitimate and documented law enforcement reason for disclosing such personal information to a law enforcement officer or civilian crime analyst.[97]

B. ALPR Systems in Canada and the UK

ALPR technology was originally developed in the UK, at Cambridge University, in response to threats from the Irish Republican Army.[98] Recently, the UK Information Commissioner found that the use of ALPR cameras at every entry

---

90. *See* Crump, *supra* note 6, at 22.

91. VA CODE ANN. § 2.2-3800 (West, Westlaw current through 2013 legislation).

92. *See* Va. Op. Att'y Gen., *supra* note 27, at 1.

93. *See* Directive No. 2010-5, *supra* note 27.

94. *See id.* at 2 ("A careful analysis of stored ALPR data can also be used to detect suspicious activities that are consistent with the modus operandi of criminals").

95. Office of the N.J. Att'y Gen., Dept. of L. & Pub. Safety, Att'y Gen. Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data (eff. Jan. 18, 2011), *available at* http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf.

96. *Id.* at 1, § 1.1.

97. *Id.*

98. Norm Gaumont, *The Role of Automatic License Plate Recognition Technology in Policing: Results from the Lower Mainland of British Columbia*, 75 THE POLICE CHIEF, no. 11, Nov. 2008, *available at* http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=1671.

and exit point to a small British city (a so-called "Ring of Steel") violated the UK Data Protection Act as being unlawful and excessive.[99]

Canadian law enforcement has also been utilizing ALPR systems since initial RCMP testing in 2006.[100] Most recently, and most relevant to the present discussion, the British Columbia Information and Privacy Commissioner (BCIPC) conducted an investigation of the use of ALPR by the Victoria Police Department (VPD) and RCMP in late 2012, concluding that certain practices violated provincial privacy law.[101] In particular, the BCIPC concluded that VPD retention of non-hit plate information, and subsequent sharing of this information with the RCMP, violated the Freedom of Information and Protection of Privacy Act (FIPPA). Importantly, the BCIPC stated that

> FIPPA authorizes the collection, use, and disclosure of personal information for a law enforcement purpose. VICPD collects personal information for the purpose of comparison against the alert listing. Once this comparison is accomplished, the authorized use of information associated with non-hits and obsolete-hits has been exhausted. FIPPA does not authorize VICPD to continue to use this information unless it obtains the consent of the individual that the information is about. VICPD is likewise not authorized to disclose this information to the RCMP.[102]

This approach, codified in British Columbian law and the equivalent federal legislation, takes significant steps toward respecting personal information privacy as the right to control access to and uses of personal information,[103] even requiring consent for the continued storage and analysis of personal information gathered in a public space. Against the backdrop of recent legal American developments in the D.C. Circuit and U.S. Supreme Court,[104] this approach will be well suited to inform the future of Fourth Amendment reform in the United States.

IV. FOR FOURTH AMENDMENT PRIVACY IN PUBLIC

A. Defining and Defending Privacy

As used throughout this paper, informational privacy is defined as the right to

---

99. Press Release, U.K. Info. Comm'r, Data Protection Act 1998 Enforcement Notice (July, 15, 2013), *available at* http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/hertfordshire-constabulary-enforcement-notice.pdf; Press Release, Info. Comm'rs Office, Police Use of 'Ring Of Steel' is Disproportionate and Must Be Reviewed (July 24, 2013), *available at* http://www.ico.org.uk/news/latest_news/2013/Police-use-of-Ring-of-Steel-is-disproportionate-and-must-be-reviewed-24072013.

100. *See* ELIZABETH DENHAM, OFFICE OF INFO. & PRIVACY COMM'R OF B.C., INVESTIGATION REPORT F12-04: USE OF AUTOMATED LICENCE PLATE RECOGNITION TECHNOLOGY BY THE VICTORIA POLICE DEPARTMENT 10-11 (Nov. 15, 2012), *available at* http://www.oipc.bc.ca/investigation-reports/1480.

101. *Id.* at 6, 29.

102. *Id.* at 6.

103. *See* arguments made *infra* Part IV.

104. *See* United States v. Jones, 132 S. Ct. 945 (2012); *see also* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

control access to and uses of personal information.[105] This definition explicitly recognizes that individuals should have some rights to control not just access to personal information, but also some subsequent uses of that information,[106] even after disclosure to third parties in certain circumstances. This definition recognizes that certain actions may waive, explicitly or impliedly, a privacy interest. Additionally, the definition is informed by the mosaic theory of the Fourth Amendment recently considered in the wake of recent decisions in *U.S. v. Jones*[107] and *U.S. v. Maynard*.[108] A person's right to limit access to and use of certain personal information (e.g., a person's current or past geographic location) that has not been kept strictly "secret" by virtue of the fact that is was available in a public space should still, in some circumstances, remain legally enforceable under the Fourth Amendment's guarantee of freedom from unreasonable search or seizure.

In essence, this is an argument for a right to privacy in certain information that, when viewed discretely or in the aggregate, is generally not qualitatively or quantitatively available to the public at large (or, as Judge Ginsburg of the Circuit Court for the District of Columbia phrased it, such information is not *actually* or *constructively* exposed to the public[109]). The aggregation of geolocation information over a substantial time period allows law enforcement to easily discover information that is both qualitatively and quantitatively different than what is knowingly and voluntarily exposed to the public at large, even though it is, in essence, just an aggregation of distinct bits of information individually exposed to the public (although tracking a person's cell phone also allows tracking when a person is inside a private building or, potentially, in the sanctity of their home,[110] which is distinctly private information).

In this pursuit, this paper will examine the proposition made by Justice Sotomayor in *Jones* that the time has come to rethink the legal significance of allowing third-party access to personal information when considering privacy interests in public spaces. By restricting the third-party rule in our Fourth Amendment analysis, such that any release of information to a third party is not necessarily a complete and total waiver to all forms of access and use by anyone at all, we respect the drastic changes in technological possibilities and their proper

---

105. *See* MOORE, *supra* note 23, at 16; Adam D. Moore, *Toward Informational Privacy Rights*, 44 SAN DIEGO L. REV. 809, 812-13 (2007).

106. MOORE, *supra* note 23, at 16.

107. 132 S. Ct. 945.

108. 615 F.3d 544.

109. *Id.* at 558 ("[U]nlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil . . . [and the] whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.").

110. *See, e.g.*, Elizabeth Dwoskin & Greg Bensinger, *Tracking Technology Sheds Light on Shopper Habits*, WALL ST. J., Dec. 9, 2013, 5:30 PM, *available at* http://online.wsj.com/news/articles/SB10001424052702303332904579230401030827722; Annalyn Censky, *Malls Track Shoppers' Cell Phones on Black Friday*, CNN MONEY, Nov. 22, 2011, 11:48 AM, http://money.cnn.com/2011/11/22/technology/malls_track_cell_phones_black_friday; Jon Brodkin, *911 Tech That Locates Cell Phone Users in Buildings Ready to Go*, ARS TECHNICA, June 6, 2013, 7:57 PM, arstechnica.com/information-technology/2013/06/911-tech-that-locates-cell-phone-users-in-buildings-ready-to-go.

role in government investigations while maintaining checks on improper abuse of authority. Defining privacy normatively in terms of control of access and use of personal information in this context can adequately protect informational privacy and balance the competing, and very important, interest in effective law enforcement.

B. Problems with Binary Fourth Amendment Theory

In the Fourth Amendment search context, legal definitions have often been crafted to force conclusions about potential privacy violations based on binary distinctions: either a form of investigation or information gathering by government agents constitutes a search or it does not.[111] This binary conceptualization of Fourth Amendment inquiry itself is not inherently problematic—in fact, it may be highly desirable. However, strictly applying the third-party doctrine—the idea that most information disclosed to some other entity attracts no legally protectable expectation of privacy—and the binary public/private dichotomy may improperly restrict Fourth Amendment protections of personal privacy, especially when considering whether individuals ought to maintain some right to privacy in public spaces.

Arguing that something "public" is, or should be, private and protected by legal rules is a difficult task. On its face, it rings of the paradoxical. Philosophical theories of privacy have primarily focused, with valid reasons, on privacy interests in sensitive and intimate information that have not been disclosed voluntarily to the public. Whether geolocation information, even when aggregated over time, should be protected is an open and controversial question. When a person, "X," steps outside of their home and walks down a busy public street, it is easy to conclude that they have waived their right to claim a privacy interest in the fact that they are walking down the street in plain view of other pedestrians, police officers, and anyone else in the near vicinity. It seems ridiculous to suggest we should "turn off our eyes." But should the fact that the eyes in the scene happen to be those of sophisticated robots or other electronic devices (drones, CCTV cameras, smartphones, Google Glass, or an ALPR camera) alter this conclusion? Or, rather than turn off our eyes (or recording devices), should we require the use of privacy-preserving technologies, such as an anti-monitoring suit[112] or device that obscures the view of nearby lenses?

It seems intuitive to argue that these bystanders cannot, and should not, be restricted from later telling someone else, including a police officer, about what they observed. Of course, this characterization assumes that we enter public spaces in a truly voluntary fashion. This might be debatable, as we often are required to pass through public spaces to supply ourselves with food or engage in work, and such a distinction would only strengthen a claim to a right to privacy in public. However, despite this important caveat, the third-party rule makes some sense insofar as it requires us to conclude that such a privacy interest has been waived in

---

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

112. Adam D. Moore, *Intangible Property: Privacy, Power, and Information Control*, *in* INFORMATION ETHICS: PRIVACY, PROPERTY, AND POWER 199, fn. 32 (Adam D. Moore ed., 2005).

these circumstances and in relation to those who also temporally occupy and share the same space—they are the primary, if not intended, "recipients" of that information. However, this situation becomes increasingly complex as we introduce various technological means of surveillance into the scene, particularly if the surveillance technologies are capable of recording data that can be easily searched and mined for relevant information years into the future, as is the case with some ALPR databases (absent the existence of more limiting data destruction polices).

Suppose we introduce a few security cameras (perhaps a variety of red light cameras, ALPR cameras, and CCTV cameras) into the street scene described above. Now, X's walk down the street is also observable by a security officer in a control room, perhaps located somewhere else entirely. If the security system is also capable of recording the video stream, the officer—or anyone else with access—can later watch, rewind, and manipulate the recording without much trouble. If the third-party doctrine (as currently interpreted) holds, the fact that X is walking down the street in view of the cameras also means that X has waived her privacy interests *vis-à-vis* the control room operator and anyone with authority to view the resulting recording. In our current technological and social climate, security cameras might not even pose the most serious threat to the permanent recording of our innocuous public meanderings, merely because they capture so little of it as a consequence of their limited placement (although whether placement is still "limited" is debatable, as levels of video surveillance have been rapidly increasing for years)[113] and individual online vigilantism, compounded with the ubiquitous nature of personal recording devices, may be increasingly likely to expose our public meanderings and embarrassing blunders.

Reverting to the earlier caveat, as we increase the duration, extent, and means of the intrusion facilitated by the various mechanisms of surveillance in the scene, are we further undermining the 'voluntariness' of a person's presence in public, and thus the idea that privacy has been waived in respect to that information? If information privacy rights revolve around the right to control access to and uses of our personal information, the additional and automatic information flow from lens to screen to hard disk to long-term archive encroaches on our right to control the use of the information for temporally restricted purposes, which has been abandoned solely because of technological intervention. At what point can, or should, our presence in public constitute a waiver of privacy rights in all potential future uses?

Many people on the street are likely carrying cell phones and other devices capable of recording video or photo, often with GPS location information built into the accessible metadata. This more recent reality introduces a sort of horizontal or non-organizational surveillance (citizens watching citizens) that has begun to breed new forms of vigilantism online. Imagine the person walking down the street is

---

113. *See, e.g.*, Hille Koskela, *'The Gaze Without Eyes': Video-Surveillance and the Changing Nature of Urban Space*, 24 PROGRESS IN HUM. GEOGRAPHY 243, 243 (2000). *See generally* Clive Norris, Mike McCahill, & David Wood, Editorial, *The Growth of CCTV: A Global Perspective on the International Diffusion of Video Surveillance in Publicly Accessible Space*, 2 SURVEILLANCE & SOC'Y 110 (2004). For just one specific example of this, see Somini Sengupta, *Privacy Fears as Surveillance Grows in Cities*, N.Y. TIMES, Oct. 14, 2013, at A1, *available at* www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html.

also carrying a smartphone. The cellular service provider is probably collecting continuous geolocational information and maintaining a database of the phone's location. Thus the service provider can make a pretty good determination of where the person is (was), which direction they are (were) walking, and at what speed they are (were) traveling. Companies like Google, Microsoft, and Apple are also providing live traffic congestion data for their electronic maps services, sourced, at least in large part, from tracking the cellphones of anyone wielding a phone running their preferred maps application or operating system. Supposedly this information is being sourced anonymously, but presumably this is based on corporate desire to avoid public outcry rather than any technological limitations, and the technological ability of law enforcement to acquire specific information from these services providers—as opposed to the wireless providers—is, as far as the author is aware, still an open question.

Additionally, the increasing effectiveness of facial recognition software, even in consumer products like Facebook, means that the capture of X's image by fellow streetwalker or CCTV camera can also lead to direct identification of X. Now, not only does X's place on the public sidewalk waive her right to privacy in the fact of her location, it could potentially mean that X has waived her right to keep her identity anonymous from anyone who might be watching, including at significant distance (or at a different time) through forms of visual surveillance enhanced by facial recognition. Any proponent of a right to anonymity in public spaces should be rightly concerned that walking the third-party doctrine to its limits in the face of advancing technology would seriously erode this aspect of privacy across society. On the other hand, increased visual surveillance of society may result in more efficient policing, crime reduction, and safer streets—although this point is challenged widely.

Returning to our example, if X concludes her walk by entering her car, parked some distance down the street in this example, and driving away, she is now susceptible to additional tracking via ALPR systems and traffic cameras installed and maintained by local police departments and departments of transportation. Even if the departments are regularly deleting the images and license plate information through automated processes, these systems promise the ability to track automobiles in real-time and save data that might be useful in active investigations. Indeed, the District of Columbia Police Department has utilized its extensive camera system to track vehicles of suspected criminals in real-time[114] and other police departments have used similar systems to gather information about when and where certain vehicles entered and left municipal boundaries or were present in certain locations near criminal incidents.[115]

The proposition that the person has waived any and all privacy interests in all of this "public" information about the person's present or historical location can still be made, but the situation is qualitatively different when the government has

---

114. Allison Klein & Josh White, *License plate readers: A Useful Tool for Police Comes with Privacy Concerns*, WASH. POST, Nov. 19, 2011, http://articles.washingtonpost.com/2011-11-19/local/35282829_1_license-plate-plates-in-real-time-tag-readers.

115. *See* Julia Angwin & Jennifer Valentino-Devries, *New Tracking Frontier: Your License Plates*, WALL ST. J., Sept. 29, 2012, http://online.wsj.com/article/SB10000872396390443995604578004723603576296.html.

such easy access to vast amounts of historical and aggregated geolocation information that can be used to determine patterns or even potentially predict future movements statistically. Of course, nothing is stopping a bystander or police officer from trailing X and recording her movements in public, as long as the trailing does not constitute harassment. However, the likelihood that an officer, or team of officers, would trail X continuously for months at a time making constant notes about precise locations and movements, including time spent at each location, was extremely low when cases like *Knotts*[116] and *Miller*[117] were decided. Presumably it remains so today.[118] Regardless, the ease with which surveillance can be conducted today makes it much less expensive and time consuming and, presumably then, more likely to occur. Rather than a team of dedicated agents tailing a suspect for weeks or months on end, a single officer need just notify a cellular service provider that locational information is needed from a particular phone (or query a large ALPR database), and pages of detailed, searchable data could be delivered almost instantaneously, alleviating the need to physically trail the suspect completely (at least for the acquisition of locational information). Increased efficiency of law enforcement investigation tactics is hardly a sound basis for requiring additional restrictions (indeed, this would be unfortunate). However, the qualitative differences in the information deemed public and the inferences that can be drawn about additional personal information suggest that certain aspects of the third-party doctrine can, and should be, critically examined.

Traditional trespass-based decisions, recently reinvigorated by the Supreme Court's decision in *United States v. Jones*, have determined whether a search has occurred on the basis of whether a property interest has been infringed by a government agent. The two-pronged *Katz* reasonable expectations of privacy test,[119] despite the allure, or dangers of its "hypothetical reasonable person" standard, has failed to modernize in pace with investigative technologies used by law enforcement around the country and remains subject to binary distinctions of legal significance, such as the public/private dichotomy and a strict adherence to the third-party doctrine or the idea that once information is released to any third-party, privacy interests *vis-à-vis* the government, when acquiring the information from the third-party, are waived. Indeed, despite calling for empirical evidence of societal expectations of privacy when examining the constitutionality of criminal investigations conducted by government agents, this hypothetical reasonable person has rarely (if ever) been a stand-in for relevant social science research on

116. United States v. Knotts, 460 U.S. 276 (1983).

117. United States v. Miller, 425 U.S. 435 (1976).

118. *See* Frank Bannister, *The Panoptic State: Privacy, Surveillance and the Balance of Risk*, 10 INFO. POLITY 65, 68 (2005) ("Physical surveillance is labour intensive and presents the state with difficult logistical and manpower problems if it is to be done on a large scale. Over the past decade developments in technology have considerably increased the scope of, reduced the cost of, and generally simplified, this process.").

119. The two-part *Katz* test requires first that an individual must have exhibited a subjective expectation of privacy and, secondly, that the expectation must be one that society is prepared to recognize as reasonable or legitimate. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

what members of the contemporary society actually expect;[120] rather courts have applied the test as a proxy for the work of social scientists and socio-legal scholars. It has been suggested that the prevalence of binary dichotomies in Fourth Amendment case law is a consequence of courts and lawyers attempting to find easy lines to draw in court.[121] However, the difficulties faced by the courts to apply the *Katz* test uniformly, problematic application of the third-party doctrine in cases involving government use of emerging technologies, and a resounding call by commentators that Fourth Amendment legal theory is in chaos (and has been for some time), suggest that the lines may not be as easy to draw at all. Perhaps the time has come to rethink Fourth Amendment theory and reduce the legal significance of some of the problematic binary distinctions that have plagued court decisions for years, such as certain applications of the third-party doctrine.

C. The Third Party Doctrine

The third-party doctrine has been described as "the Fourth Amendment rule scholars love to hate."[122] For years, it has been subjected to voluminous amounts of criticism, both by legal scholars and state courts.[123] The Supreme Court has upheld the rule, holding that citizens "assume the risk" that what they disclose to a third party will be transferred on to the government, but has not explicitly defended it.[124] And now, after *Jones*, criticism of the rule has reached the Supreme Court itself.

In its early years, the third-party doctrine was applied in cases involving undercover agents and confidential informants.[125] These cases held that defendants could not claim Fourth Amendment violations based off of conversations with government agents—sometimes wearing wires—because the "the Fourth Amendment does not protect 'a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.'"[126] In later cases, the Court applied the doctrine to business records. In *United States v. Miller*, the Supreme Court held that a bank depositor does not have any reasonable expectation of privacy in financial information (in the form of deposit slips, checks, and bank records) because such information was conveyed voluntarily to the bank and "exposed to their employees in the ordinary course of business."[127] As such, the court found that

> [t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the

120. For a discussion of prior empirical work and the court's (non)use of the relevant empirical findings, see Jeremy A. Blumenthal, Meera Adya, & Jacqueline Mogle, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U. PA. J. CONST. L. 311 (2009).

121. Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 647 (2013).

122. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

123. *Id.* at 563-64.

124. *Id.* at 564.

125. *Id.* at 567.

126. *Id.* at 568 (quoting Hoffa v. United States, 385 U.S. 293, 302 (1966)).

127. United States v. Miller, 425 U.S. 435, 435 (1976).

> confidence placed in the third party will not be betrayed.[128]

In her concurrence in *Jones*, Justice Sotomayor stated that the time had come for Fourth Amendment jurisprudence to discard the premise that legitimate expectations of privacy could only be found in situations of near or complete secrecy.[129] Sotomayor argued that people should be able to maintain reasonable expectations of privacy in some information voluntarily disclosed to third parties. The opposite and historical view of the court, Sotomayor stated, was "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[130] Sotomayor considered that logs of phone calls, text messages, websites visited, email correspondence, purchase histories from online retailers, and geolocational information were all forms of information that were technically disclosed to third parties through mundane tasks, but where such disclosure should not constitute waiver of all privacy interests.[131] "[W]hatever the societal expectations," Sotomayor stated, these forms of information

> can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[132]

However, discarding the idea behind the third-party doctrine completely seems ludicrous. Intuitively, what a person exposes to the public is just that—public. It loses its status as private information exactly because a person voluntarily puts it in the public view. To hold otherwise in all cases might seriously undermine free speech and other important Constitutional guarantees. Certain applications of the doctrine are not necessarily troublesome. For example, the suggestion that an officer may tail a suspect while on public roads without first obtaining a warrant seems entirely reasonable. After all, the information gained by the officer by physically following the suspect is precisely what the suspect has openly and voluntarily exposed to the public at large. Extending this doctrine, we can conclude that an officer (or likely a large team of officers) should be allowed to tail a suspect continuously for weeks at a time, all the while making copious notes about the suspect's movements and locations in publicly accessible spaces.

What, then is the problem with allowing the officer to utilize a more efficient means of gathering the same information, namely through contacting the suspect's wireless provider and getting a log of geolocational data related to the suspect's phone (which has presumably remained near the suspect)? This question is a difficult critique of the position I present in this paper, but I believe it can be overcome. I also do not feel that my argument is aimed at hindering the efficiency of law enforcement work without solid philosophical grounds. As stated by Justice Sotomayor, the situation with prolonged geolocational tracking is different

---

128. *Id.* at 443 (citations omitted).
129. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).
130. *Id.*
131. *Id.*
132. *Id.*

precisely because the technological surveillance "evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility'"[133] and allows the government to obtain personal information about individuals that is qualitatively and quantitatively different in kind than what would be discovered alternatively. The likelihood that, in the case of physical tailing, such a time consuming and resource-intensive investigation would be carried out regularly without a sound basis is very small. Police are very unlikely to devote such time and resources to this kind of visual surveillance except in cases that really warrant it. On the other hand, the ease and convenience of obtaining records from wireless providers could allow government agents virtually unfettered ability to conduct this sort of surveillance in a wide variety of cases, including "fishing expeditions" not based on any level of suspicion, probable cause or otherwise. However, this position could potentially limit some important investigations from proceeding as efficiently as they might have based purely on departmental lack of resources to conduct extensive visual surveillance. But requiring a warrant, based on affirmation of probable cause, before allowing government agents to collect and analyze such extensive digital information, should not be a serious impediment to most investigations and would help restrict this sort of surveillance to legitimate investigations. Additionally, other exceptions to the Fourth Amendment's warrant requirement, such as the emergency doctrine,[134] would continue to ameliorate these concerns in practice when time is of the essence.

However, by limiting a strict application of the third-party doctrine, new questions emerge about where lines should be drawn between permissible and impermissible tactics in other contexts. For example, what are the important differences—if any—between aggregating geolocational information, bank records, "private" communication or messages on a social network like Facebook, web browsing or search histories, or electronic purchase histories collected and archived over time? The mosaic theory, originally announced by Judge Ginsburg in *U.S. v Maynard*, may begin to help us sort out these difficult questions.[135]

D. Public Surveillance, the Mosaic, and the Fourth Amendment

Some scholars have claimed that recent (and even not so recent) advances in digital technologies and surveillance capabilities mean that we should rethink whether we can maintain any legitimate expectations of privacy while out in public—or in "public facts." In *Jones*, Justice Sotomayor proposed that the third-party doctrine should be abandoned (or at least rethought) in the face of confronting Fourth Amendment challenges related to investigative use of new

133. *Id.* at 956 (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

134. United States v. Goldenstein, 456 F.2d 1006, 1009 (8th Cir. 1972); *see also* Melinda Roberts, *The Emergency Doctrine, Civil Search and Seizure, and the Fourth Amendment*, 43 FORDHAM L. REV. 571, 571 (1975).

135. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012) ("As with the 'mosaic theory' often invoked by the Government in cases involving national security information, 'What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene.'" (quoting CIA v. Sims, 471 U.S. 159, 178 (1985) (internal quotation marks omitted)).

technologies.[136] Justice Alito's separate concurrence in *Jones* expressed concern about the robustness of the "reasonable expectations of privacy test"—even while advocating its use in that case—because of the potential that the widespread use of new surveillance technologies could resign the populace to subjectively expect less privacy than should be afforded under the Constitution.[137] Indeed, geolocational tracking technologies—which have now been used by law enforcement agencies for some time—allow law enforcement to easily compile thousands of pages of information about our present and past travels—in very exacting detail—and to mine that information indiscriminately for patterns.[138] Courts have also clearly stated that Fourth Amendment law has failed to keep pace with advancing technological possibilities. In one recent Ninth Circuit case, the court stated that

> [t]he extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question. The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored.[139]

Prior to Jones, the precedential locational tracking case was *United States v. Knotts*.[140] In that case, the Court held that police use of a "beeper"—a much more rudimentary and non-exact form of tracking a suspect by radio transmissions[141]did not violate the Fourth Amendment because a person does not have a reasonable expectation of privacy in their movements on a public road.[142] Police placed the beeper at issue in a container of chloroform prior to codefendant Petschen's purchasing the container and placing it in his car. The court stated that

> [v]isual surveillance from public places along Petschen's route or adjoining Knotts' premises would have sufficed to reveal all of these facts to the police. The fact that the officers in this case relied not only on visual surveillance, but on the use of the beeper to signal the presence of Petschen's automobile to the police receiver, does not alter the situation. 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.[143]

This decision grants the government the authority to amplify, or replace, their own visual surveillance of a suspect moving in public spaces on the rationale that all of the surveillance could have been done lawfully by actual officers tailing and observing the suspect's movements. However, it also did more than just augment visual possibilities, despite the comparatively limited information produced by the beeper as compared to modern GPS tracking technologies. For example, at one

---

136. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

137. *Id.* at 962-63 (Alito, J., concurring).

138. In *Jones*, for example, prosecutors presented over 2,000 pages of data about Jones's location over a 28 day period sourced from a physical tracking device installed in the rear bumper of a vehicle Jones regularly drove. *Id.* at 948.

139. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008).

140. United States v. Knotts, 460 U. S. 276 (1983).

141. *See id.* at 277.

142. *Id.* at 282.

143. *Id.*

point the officers in *Knotts* lost sight of the car they were tailing and subsequently fell out of range of the beeper, effectively losing their target.[144] They later found the device using a helicopter to sweep the area scanning for the beeper's signal and located the device near a cabin occupied by Knotts.[145] This use of the location tracking technology did more than simply augment the sensory capabilities of the officers—it allowed them to locate a suspect using purely technological means after visual tracking had failed. More recently, the facts of the *Jones* and *Maynard* cases provide stark contrast to the limited technological capabilities and judicial reasoning in *Knotts*.

In 2004, Lawrence Maynard managed a nightclub in the District of Columbia owned by Antoine Jones. That year, an FBI-Metropolitan Police Department task force began investigating Jones and Maynard (and several other alleged co-conspirators) for narcotics violations. During the course of the investigation, officers conducted visual surveillance of the nightclub, installed a video camera focused on the front door of the club, and captured pen register information and instituted a wiretap of Jones's cellular phone.[146] Based on information gathered during this initial surveillance, the officers applied for and obtained a warrant to place an electronic GPS tracking device on an automobile regularly used by Jones (but registered to his wife).[147] The warrant authorized the government to install the device on the vehicle within the District of Columbia within a ten-day time period. Eleven days later, the officers installed the device while the vehicle was in Maryland in violation of the terms of the warrant—a claim the government admitted to in the litigation, while still maintaining that a court order was not required by law in the first place. Eventually, Maynard and Jones were tried jointly and convicted of various drug related offenses. On appeal, the Circuit Court for the District of Columbia reversed Jones's conviction based on his claim that the government's warrantless GPS tracking of his vehicle 24 hours a day for 28 days violated his Fourth Amendment rights.[148] Importantly, while announcing the "mosaic theory," the court found that

> unlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil… [and] the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.[149]

The court compared this case of prolonged modern surveillance with prior national security cases where the government regularly invoked the "mosaic theory" to shield certain otherwise public records from disclosure under the Freedom of Information Act because, "[w]hat may seem trivial to the uninformed,

144. *Id.* at 278.
145. *Id.*
146. United States v. Jones, 132 S. Ct. 945, 948 (2012).
147. *Id.* at 949.
148. United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010).
149. *Id.* (emphasis in original).

may appear of great moment to one who has a broad view of the scene."[150] The court continued by stating that

> [p]rolonged 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. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[151]

This concern was later voiced loudly by the Justices in the Supreme Court's decision in *Jones*, which upheld the decision of the Circuit Court.

Combining the third-party doctrine with the modern realities of massive data collection made possible because of the ubiquitous nature of contemporary communications devices means that location data, even historical data, is becoming much easier for law enforcement to obtain without the need to secure a warrant supported by probable cause, even without planting physical devices and risking committing physical trespass. Indeed, the police in *Jones* did obtain historical geolocation information from Jones's wireless provider, but chose to rely on the data collected through a physical tracking device installed on Jones's vehicle during the trial. The present ability of law enforcement to so easily amass and mine such enormous amounts of personal information through simple technological tools and coordination with service providers (such as wireless service providers, email providers, or social network service providers) begs an examination of current Fourth Amendment theory, the reasonable expectations of privacy test, and the third-party doctrine.

E. The "Mosaic Theory" of the Fourth Amendment

Underlying the "mosaic theory" is the idea that the courts can sometimes consider the information gathered through government surveillance (or presumably the surveillance activities of government agents—depending on where we draw the line) in the aggregate when deciding when a "search" for Fourth Amendment purposes has occurred, rather than being required to focus sequentially on each distinct piece of information or government act.[152] The theory was introduced by Justice Ginsburg in *United States v. Maynard*, the decision by the D.C Circuit that led to the Supreme Court's decision in the *Jones* case. In his opinion, Judge Ginsburg introduced the mosaic standard, focusing on whether the government's

150. *Id.* at 562 (quoting CIA v. Sims, 471 U.S. 159, 178 (1985) (internal quotation marks omitted)).
151. *Id.* at 562.
152. *See generally* Kerr, *supra* note 111.

investigation caused them to learn "more than a stranger would have observed."[153] Early commentary has resulted in both academic praise and criticism of the idea of a mosaic theory. Potentially, considering this information, and government surveillance practices, in the aggregate could help modernize existing theory, and reflects a pragmatic approach to respecting forms of informational privacy that would comport with legitimate expectations of privacy despite not necessarily being consistent with existing Fourth Amendment jurisprudence. Critics express concern that implementing this new theory would throw Fourth Amendment law into deeper chaos and will require the courts to confront an expansive array of practical questions and draw more arbitrary lines without precedential guidance.[154]

Prior to the recent judicial consideration the mosaic theory by the D.C. Circuit and Supreme Court, searches have been determined by what Orin Kerr calls the "sequential approach."[155] Under this approach, courts "analyze whether government action constitutes a Fourth Amendment search or seizure [by taking] a snapshot of the act and assess[ing] it in isolation."[156] According to Kerr, the "step-by-step" or "frame-by-frame analysis" is inherent in and foundational to evaluating Fourth Amendment claims.[157]

However, in Maynard, the Circuit Court "likened the aggregate of Jones's movements to a mosaic, where the whole is more than the sum of its parts."[158] Justice Ginsburg imported the theory from cases where Freedom of Information Act requests were weighed against national security interests because "[d]isparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information."[159] Thus, according to Justice Ginsburg, the difference between the whole array of potentially public information and any distinct part "is not one of degree but of kind."[160] Access to the whole set of documents could allow enemies to ascertain or infer additional private information. Such it is with geolocational information and the present ability of law enforcement to track individuals comprehensively for weeks on end without any physical trailing. Apparent support for these ideas at the Supreme Court may signal an opportunity to reform the Fourth Amendment analysis in such a way that provides important protections for personal information control in a world of quickly advancing technology and rising risks of improper access to growing amounts of personal information stored in electronic computer databases.

F. Finding a Legal Basis for Privacy in Public

Since Justice Harlan announced a two-part test in a concurring opinion in *Katz*

153. *Id.* at 330.

154. *See, e.g.*, *id.* at 314-15.

155. *Id.* at 314.

156. *Id.* at 315.

157. *Id.* at 316.

158. Bethany L. Dickman, Note, *Untying Knotts: The Application of Mosaic Theory to GPS Surveillance in United States v. Maynard*, 60 AM. U. L. REV. 731, 736 (2011).

159. David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 630 (2005).

160. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

v. United States[161] in 1967, whether or not a person maintains a right to privacy—for Fourth Amendment search purposes—is based on whether any subjective expectation of privacy maintained by the individual asserting the privacy interest is "one that society is prepared to recognize as reasonable."[162] Generally in the United States, courts have found that information released to the public could not be the subject of any legitimate expectation of privacy under this test. From 1967 until the *Jones* decision in 2012, the reasonable expectation of privacy test largely succeeded the prior focus on whether the government has violated a property right, such as by committing trespass, in conducting a search. Justice Scalia's majority opinion in *Jones*, however, reinvigorated the trespass doctrine for searches where physical trespass had occurred, while allowing for the continued use of the *Katz* test when non-trespassory interests are allegedly violated. In *Jones*, the court held that unwarranted placement of a GPS tracking device by the government on a vehicle frequently used by the defendant, a suspected drug trafficker, violated the Fourth Amendment because the officers committed a trespass by physically attaching the device to the vehicle. This opinion left open the Fourth Amendment question for searches conducted without any physical trespass, such as when the government tracks a cell phone's location electronically. Additionally, the justices were writing in response to the lower court's decision by Judge Ginsburg of the D.C. Circuit that espoused the so called "mosaic theory"—the idea the certain government investigation tactics, such as tracking suspects via GPS devices or geolocation data provided by cellular phone service providers (or, presumably, other forms of data mining a wide variety of electronic records and online information), empowered the government to accumulate such a detailed digital picture of a person's life, routines, habits, and travels that the information gathering itself triggered Fourth Amendment protection, despite the fact that a search for any individual piece of the same data might not have done so because the information was in some sense publicly available. In her concurrence, Justice Sotomayor expressed her worries that this sort of technologically enhanced investigation changed the balance at the heart of the Fourth Amendment.

> In cases involving even short-term monitoring . . . GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility."[163]

Despite the radical shift that such dicta might indicate for the future of Fourth

---

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

162. *Id.* at 361 (Harlan, J. concurring).

163. United States v. Jones, 132 S. Ct. 945, 955-56 (2012) (Sotomayor, J., concurring) (citations omitted); *see, e.g.*, People v. Weaver, 909 N.E. 2d 1195, 1199 (N.Y. 2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.").

Amendment doctrine, Justice Sotomayor's call for greater protections for some activity occurring in the public sphere is not the first time the idea has been suggested in the courts. In the *Katz* decision itself, Justice Stewart stated that

> [w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, *even in an area accessible to the public*, may be constitutionally protected.[164]

In that case, the government had placed a listening device to the exterior of a public phone booth, and had recorded the defendant making phone calls. The court found that Katz maintained a reasonable expectation of privacy in his conversations while inside the phone booth, even though it was in a public place, because the court felt that

> a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the *vital role that the public telephone has come to play in private communication*.[165]

The court continued its "discrediting" of the view that only trespass could raise constitutional questions, elaborating that

> once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.[166]

Reading this language alongside Sotomayor's concurrence in *Jones*, parallels begin to emerge. The expectation that shutting the glass door to a public phone booth makes the conversation private is entirely consistent with the proposition that emails sent to an associate, purchase histories shared only with the online merchant, geolocational information shared only with a cellphone service provider, or a social networking status update visible only to a select groups of friends (due to actively setting and maintaining privacy settings to ensure such limited publication), could also be considered legitimate contexts where a reasonable expectation of privacy vis-à-vis the government could adhere.[167] However, the historical reliance on the third-party doctrine would presumably discredit these otherwise reasonable expectations merely because the information was disclosed to an intermediary (e.g., Google, Facebook, Verizon, T-Mobile, Amazon) or a select group of friends. Thus, the government is free to demand and subpoena this information from these intermediaries without obtaining a warrant or attesting to probable cause in court. However, the "vital role" that the public telephone played in facilitating private communication (even in public spaces) in 1967 has been superseded by a variety of electronic wireless communications technologies (e.g.,

---

164. *Katz*, 389 U.S. at 351 (emphasis added) (citations omitted).
165. *Id.* at 352 (emphasis added).
166. *Id.* at 353.
167. *See* Newell, *Rethinking Reasonable Expectations of Privacy*, *supra* note 5.

cell phones, email, text messaging, and private messaging on social media websites) that also collect and transmit a wealth of data (such as geographic coordinates) that find no easy corollary in the *Katz* analogy.

Some lower federal courts have begun to question a strict application of the third-party doctrine as well. In 2010, the Sixth Circuit addressed the question of whether the government violated the Fourth Amendment when agents compelled an ISP to turn over the contents of the defendant's emails without first obtaining a warrant.[168] In that case, the Sixth Circuit held that, even though the subscriber agreement allowed the ISP to access the contents of its clients' emails in certain circumstances, "the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."[169] The court found that this conclusion was consistent with the *Katz* holding, because the telephone service company in the prior case also had a legal right to listen to phone calls in certain cases. The *Warshak* court also differentiated the facts in that case from those in *Miller*, because the third-party ISP was merely an intermediary rather than the intended recipient (as the bank was in *Miller*). Under the rationale in this case, the government could not demand the information from the intermediary corporation or service provider, but the conclusion would not necessarily extend to information released by the recipients of the communication, such as the email recipient or Facebook friend. Whether this was the right result, or merely a step in the right direction, remains the subject of some controversy. However, as evidenced by the recent indication by the five concurring justices in *Jones* (Sotomayor was the most explicit, but Alito's opinion can also be read this way) that they may be willing to rethink Fourth Amendment theory,[170] the time may be ripe for further challenges to precedent. Indeed, the fact that the *Jones* decision followed from the introduction of the mosaic theory in the lower court's decision signals that the justices may be willing to entertain this issue in coming years.

The recognition of the Court in *Katz* itself of this relationship between the Fourth Amendment, private communications, and technological change, provides ample support for the proposition that these new forms of private communication (and the variety of additional opportunities they provide, both to government and individuals) should be carefully protected as well. This analysis is more problematic, however, when applied to geolocational information, which is not clearly a form of communication but more like a public fact. The mosaic theory provides one way to sidestep this concern, focusing on the qualitative difference between visual confirmation of a person's location and the vast history of geolocational data potentially stored by—or accessible to—law enforcement through modern tracking technologies, while preserving the idea that new technologies should receive carefully considered protections under the Fourth Amendment.

---

168. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

169. *Id.* at 286.

170. Christopher Slobogin, *Making the Most of Jones v. United States in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 1-2 (2012) ("[A]ll three opinions in *Jones* made statements that call into question the Court's 'third party doctrine.'").

V. EXPLORING THE SPD ALPR DATABASES

The following section describes the nature of what is contained in the two databases disclosed by the SPD under state FOI law. The first database (the "PIPS Database") consists of ALPR cameras mounted on SPD patrol cars. It is the larger of the two databases in terms of number of scans recorded, with over 1.5 million license plate scans recorded over a period of 87 days from January to April 2013. The second database (the "AutoVu Dabatase) contains fewer scans, at just over 275,000 during a 77-day period from December 2012 to February 2013, but also includes photographs of the vehicles scanned (the PIPS database maintained by SPD does contain photos, but they were not disclosed in this case). Each database contains un-redacted license plate numbers from the scanned vehicles, officer login IDs, timestamps, latitude and longitude of each scan, as well as other information about which scans resulted in hits.

Because the databases overlap in time (from January 9 to February 15, 2013) they give a fairly accurate depiction of how the two systems were used and deployed during that time period. Consistent with numbers reported by other agencies to the ACLU,[171] these databases indicate that hits occurred only a fraction of the time (combined, at 1.2 percent of total scans). Interestingly, the larger PIPS Database recorded a hit only 25 times every 10,000 scans. The two systems have been incredibly active, scanning an average of 20,865 license plates every day over the represented time periods. On January 9, 2013, one officer alone scanned over 7,000 plates in a single shift. Together, these mobile systems canvassed a large portion of the city, as represented in Figure 1, *infra*, although certain neighborhoods remained remarkably under-scanned in comparison.

Database	SPD PIPS (patrol car) Database	SPD AutoVu (parking enforcement) Database	Totals
Date range of scan data:	01.09.2013 – 04.05.2013	12.01.2012 – 02.15.2013	-
No. of days in database:	87	77	-
Total no. of scans:	1,501,547[172]	277,718	1,779,265
Avg. scans per day:	17,259	3,606	20,865
Total no. hits:	3,775	5,885	9,660
Avg. hits per day:	43.4	76.4	119.8
Percent of scans as hits:	0.25% (less than 1%)	2.1%	1.2%

Tbl. 1 – Overview of both SPD databases.

171. *See* Crump, *supra* note 6, at 13.

172. This total excludes one removed line, which was filled with NULL in each column; other system reads not excluded, so this number may be a little high for actual license plate scans.

Not every scan returned accurate geolocation coordinates for the location the scan occurred, although most did (76.5 percent for PIPS; 99.9999 percent for AutoVu). On average, the PIPS system also calculated an 87 percent confidence rate in the optical character interpretation, rising to 91 percent for scans resulting in hits. Because each database contains information about individual officer logins (41 unique login IDs in the PIPS system; 91 in the AutoVu system), and many of these officers scan hundreds or thousands of cars in any given shift, the time and location of each scan paints a very accurate picture of officer movements over time.

Fig. 1 – Mapped ALPR data from SPD ALPR Databases (cropped to include only Seattle city limits). On the left, the larger PIPS database, from cameras mounted on SPD patrol cars. On the right, the SPD AutoVu database, mounted on parking enforcement vehicles.

Fig. 2 – Mapped ALPR data from SPD ALPR Databases (cropped to include only downtown Seattle). On the top, the larger patrol car database. On the bottom, the SPD parking enforcement database.

Additionally, the databases indicate that multiple SPD officers scanned plates outside the Seattle city limits, and one scanned passing plates into the relatively distant cities of Snohomish, Port Orchard, and Fife.[173] Other officers scanned plates in Burien, Washington, and onto Bainbridge Island (including scanning plates while on the ferry between Seattle and Bainbridge). Because of the detailed

173. Another, larger ALPR database from an earlier period obtained by the ACLU of Washington State also includes scans outside of Washington State, when an officer scanned plates all the way into Portland, Oregon.

nature of the data, it is possible to calculate an officer's rate of speed, determine which exits were taken and at what times. This information has numerous uses to determine whether the systems are being used in appropriate ways, and raises a host of interesting questions related to privacy (of the officers and of innocent citizens, including those scanned in areas outside SPD jurisdiction).

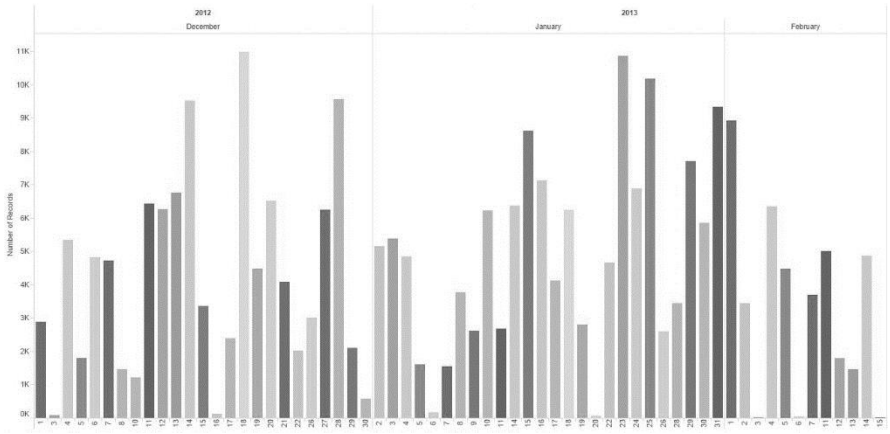

Fig. 3 – Number of ALPR scans on a daily basis from Dec. 1, 2012 to Feb. 15, 2013, as contained in the SPD AutoVu Database. Number of days with no scan data: 14. High: 10,994 scans on Dec. 18, 2012.

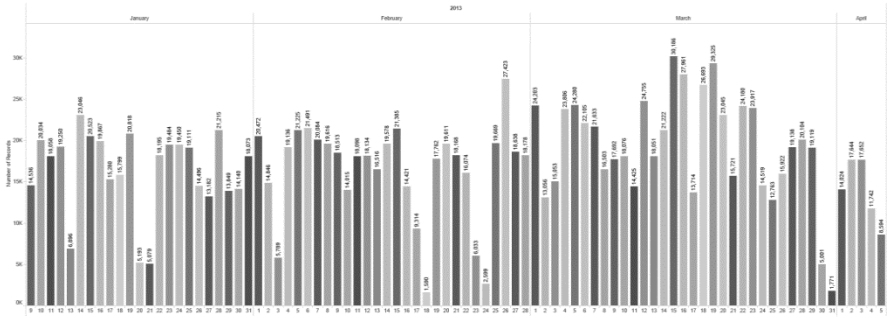

Fig. 4 – Number of ALPR scans on a daily basis from Jan. 9, 2013 to Apr. 5, 2013, as contained in the SPD PIPS Database. Number of days with no scan data: 0. High: 30,186 scans on Mar. 15, 2013.

Even a single day of data can lead to interesting exploratory findings and provide a glimpse of how the systems are utilized throughout the city. Tables 2 and 3, below, present scanning data from both databases on a single day, January 23, 2013. Figure 5, below, presents graphically the geographic coordinates of each scan created by two of the SPD patrol cars on the same date.

User/Login	# Scans	# Hits	% Hits	Scanning Time	Hours	Scans per hour
A	6840	18	0.3%	6:23am – 4:11pm	9:48	698
B	5757	13	0.2%	5:34pm – 11:59pm	6:25*	896.7
C	811	2	0.2%	12:00am – 2:55am	2:55*	278.1
(two shifts)	1046	3	0.3%	7:58pm – 11:59pm	4:01*	260.4
D	1687	5	0.3%	11:48am – 7:47pm	7:59	211.3
E	848	0	0.0%	12:34pm – 6:49pm	6:15	135.7
F	807	2	0.2%	8:32pm – 11:43pm	3:11*	253.5
G	752	1	0.1%	12:25pm – 7:34pm	7:09	105.2
H	428	6	1.4%	7:42pm – 11:56pm	4:14*	101.1
I	221	0	0.0%	12:02am – 12:37am	0:35*	379.1
J	152	0	0.0%	12:10am – 3:35am	3:25*	44.5
K	128	0	0.0%	1:49am – 3:15am	2:26 *	52.7
L	7	5	71.4%	8:49am – 1:13pm	4:24	1.6
Totals	**19484**	**55**	**0.28%**	**-**	**62:47**	**310.3**
Total (all days in db)	1,501,547	3773	0.25%	-	-	-
*** Partial shift. Additional scans take place prior to, or after, 12:01am or 11:59pm on Jan. 23, 2013**						

Tbl. 2 – Scan data for scans on January 23, 2013 (PIPS Database)

Unit	# Scans	# Hits	% Hits	Scanning Time	Hours	Scans per hour
1	3814	99	1.9%	7:21am – 2:36pm	7:15	529.7
	134			4:42pm – 5:01pm	0:19	
	447			8:25pm – 9:43pm	1:18	
	779			11:00pm – 11:54pm	0:54*	
2	4000	45	0.8%	7:56am – 3:08pm	7:12	472.8
	645			4:47pm – 5:44pm	0:57	
	1052			7:59pm – 11:53pm	3:54*	
Totals	**10,871**	**144**	**1.3%**	**-**	**21:54**	**496.4**
Total (all days in db)	277,718	5,885	2.1%	-	-	-
*** Partial shift. Additional scans take place prior to, or after, 12:01am or 11:59pm on Jan. 23, 2013**						

Tbl. 3. – Scan data for scans on January 23, 2013 (AutoVu Database). Broken out when breaks > an hour.

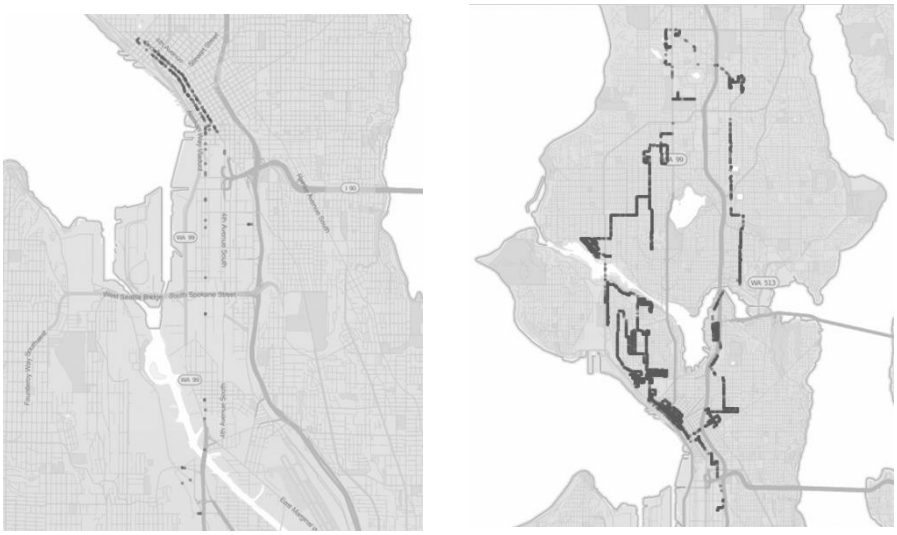

Fig. 5 – Scans on January 23, 2013 by individual scanning units. From PIPS database. User/Login (correlated to the randomized identifiers from Table 2, above) "I" on the right (n=221); "B" on the left (n=5757).

VI. ALPR DATA AS PUBLIC RECORD

Because information can provide and facilitate power, the collection and use of large amounts of information (including ALPR data) can significantly impact the relationships between governments and their citizens.[174] Access to information about government activities is often a prerequisite to gaining and exercising power or seeking redress for potential rights violations stemming from secret activities of others.[175] The openness of the SPD, evidenced by their willing disclosure of detailed ALPR databases stands in sharp contrast to states where statutes now restrict public access to this type of data, such as in Minnesota, Maine, Arkansas, Utah, and Vermont. In these jurisdictions, this willingness to allow government surveillance (albeit with varying limitations) and limit citizens the rights of reciprocal surveillance, represents a potential imbalance in power between citizens and their governments. This imbalance has the ability to tip the scales of power and limit the ability of the people to exercise democratic oversight and control those they have put in power to represent them.[176]

As stated by the California Supreme Court,

> it has long been apparent that the desire for privacy must at many points give way before our right to know, and the news media's right to investigate and relate, facts about the events and individuals of our time.[177]

---

174. *See* CRAIG FORCESE AND AARON FREEMAN, THE LAWS OF GOVERNMENT: THE LEGAL FOUNDATIONS OF CANADIAN DEMOCRACY 481-84 (2005).

175. *Id.*

176. *Id.*

177. Shulman v. Group W Prods., 955 P.2d 469, 474 (Cal. 1998).

Freedom of information (FOI) laws have provided a great deal of access to government records in recent years, and they serve as a powerful and effective means for empowering oversight by journalists and ordinary citizens. In a very real sense, these laws provide a legal mechanism for citizen-initiated surveillance from underneath (sometimes termed "sousveillance"[178] or the "participatory panopticon"[179]). This form of reciprocal surveillance (which may take numerous forms, including public access to ALPR data generated by the state or local governments) grants citizens greater power to check government abuse and force even greater transparency.[180] Edward Snowden's decision to leak classified NSA intelligence documents to the press in 2013 certainly reinvigorated national and international critique of large-scale surveillance programs, but the controversies are not really all that new. And they do not exist solely at the level of national intelligence.

VII. CONCLUSION

As government agencies and law enforcement departments increasingly adopt big-data surveillance technologies as part of their routine investigatory practice, personal information privacy concerns are the obvious jumping-off point for critique and media coverage. However, law enforcement goals of more effective and efficient policing to keep our streets and communities safe are also weighty values that must be balanced against privacy concerns. How to strike the right balance is, of course, a tricky question that will no doubt attract much scholarly ink in the years to come. In the context of ALPR use, though, this paper advances a few normative claims.

First, we must strike a balance between allowing large-scale ALPR deployment and the privacy rights of individual citizens. Second, we must also strike a balance between personal privacy and granting access to government information, such as ALPR databases, since the disclosure of un-redacted license plate information (as well as enough geolocational coordinates) can be easily tied to an individual person, address, or place of business. Public access to this data also risks officer privacy, and limiting access would eviscerate the public's ability to conduct certain types of oversight made possible by access to detailed officer movements. Despite all these competing interests, a few conclusions seem apparent, given the obvious biases expressed throughout this paper. These conclusions do limit public access, but they do so to preserve the privacy rights of

178. *See* Steve Mann, Jason Nolan, & Barry Wellman, *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, 1 SURVEILLANCE & SOC'Y 331 (2003), *available at* http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3344/3306; Jean-Gabriel Ganascia, *The Generalized Sousveillance Society*, 49 SOC. SCI. INFO. 489 (2011).

179. Jamais Cascio, *The Rise of the Participatory Panopticon*, WORLD CHANGING (May 4, 2005), http://www.worldchanging.com/archives/002651.html; Mark A. M. Kramer, Erika Reponen & Marianna Obrist, *MobiMundi: Exploring the Impact of User-Generated Mobile Content—The Participatory Panopticon*, *in* PROCEEDINGS OF THE 10TH INTERNATIONAL CONFERENCE ON HUMAN COMPUTER INTERACTION WITH MOBILE DEVICES & SERVICES 575-77 (2008).

180. *See generally* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998); KEVIN D. HAGGARTY & RICHARD V. ERICSON, THE NEW POLITICS OF SURVEILLANCE AND VISIBILITY 10 (2007).

innocent citizens (and, as a consequence, also protect the privacy of individual police officers).

As a first step, we ought to limit data retention on non-hit scans in a reasonable amount of time, as indicated by the BCIPC's report to the VPD. This would have two consequences: 1) it would protect the privacy of innocent citizens (those whose plates are not legitimately on any law enforcement hotlist) by limiting the ability of the police to conduct after-the-fact analysis of these individuals' historical movements and, 2) it would limit the ability of anyone to track an officer's precise movements with such great accuracy. There are two potential options for this solution: either we require non-hot data to be purged from the database within a reasonable amount of time (in British Columbia, for example, VPD is required to redact this information at the end of every shift, prior to sharing data with the RCMP) or we require the anonymization of non-hit entries in the database (e.g., redacting or randomly altering license plate numbers from the data).

Due to fears of re-identification, we might promote the first option: complete redaction. This option preserves the privacy of innocent motorists as well as the individual officers. On the other hand, this option also significantly limits the citizens' ability to monitor officer use of these systems as only a small fraction of the overall scans would remain, giving a much less accurate picture of policing patterns. The second option would maintain a larger corpus of data, for use both by citizens and the police departments themselves, facilitating data-driven and predictive policing efforts as well as citizen oversight, but does so at the risk of re-identification. For present purposes, without a more detailed analysis of the re-identification risks involved, either of these options represents a drastic improvement in general practice, especially as these practices are exhibited in the Minneapolis and Seattle cases.

As a second, and absolutely necessary, step, such anonymized ALPR data should not be exempted from public disclosure. This normative claim supports vital interests in government transparency, regardless of whether we opt for redaction or anonynmization. This policy would allow some oversight through public disclosure, and would allow the public to conduct an informed debate about the efficacy and cost of the use of these systems in their communities.

This conclusion, bifurcated into two potential options, admittedly does not answer the final balancing question completely. Option one does more to protect privacy than it does to force a right to reciprocal surveillance, and the second option preserves this right at the risk of re-identification. Neither is therefore perfect, but both are better than what generally exists at present. Importantly, there are strong reasons to push back against the trend to pull a curtain of secrecy over ALPR data all together. This privacy-weighted conclusion is warranted, to some degree, by the importance of recognizing greater rights of privacy in public spaces, especially when it concerns subsequent aggregation and data-mining of otherwise innocent peoples' personal information. Modern surveillance technologies make it incredibly easy for government agents to track individual citizens discretely and comprehensively for very long periods of time. Court decisions finding that citizens do not maintain legitimate expectations of privacy in their public movements and strict application of the third-party doctrine to aggregated forms of government information gathering need to be rethought and critically examined in

light of modern technological advances. The unrestricted ability of law enforcement to engage in mass amounts of geolocational surveillance that captures the personal information of innocent individuals, including the use of ALPR, threatens individual privacy and bypasses traditional checks on abusive government actions. The nature and amount of data available about most people's movements—both present and long into the recent past—allows law enforcement to draw inferences about other personal information, and should be subject to the probable cause warrant requirement of the Fourth Amendment. The mosaic theory provides one useful lens and framework for analyzing these sorts of cases. It also "protects the Fourth Amendment from innocuous erosion by society's ready adoption of such technology" even as governmental "use of GPS devices becomes a social norm."[181]

On the other hand, advancing technologies and data-mining potentially offer law enforcement greater ability to detect, investigate, and prosecute criminal activity. These concerns for personal information privacy and the efficacy of law enforcement are both very important in contemporary society. The tensions between these two legitimate aims is substantial and, in the context of police use of automated license plate recognition (ALPR) systems, limiting the scope of law enforcement data retention to protect citizen privacy might also protect the privacy of the police officers using these systems. Thus, we can serve the interests behind FOI laws, including the implicated First Amendment rights to gather information about government conduct, and personal privacy rights by limiting long-term retention and the sharing of any non-hit license plate information with other agencies or private companies. The recent practice of the Seattle Police Department demonstrates an applaudable commitment to transparency and, combined with more limited data retention, as described above, would provide a compelling example for managing the risks and benefits of ALPR use.

181. Dickman, *supra* note 158, at 738.