



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ALPR EXPANSION PROGRAMS AND DATA PRIVACY

by

Aaron J. Zeigler

December 2023

Co-Advisors:

David W. Brannan (contractor)
Anshu N. Chatterjee

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE December 2023	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE ALPR EXPANSION PROGRAMS AND DATA PRIVACY			5. FUNDING NUMBERS	
6. AUTHOR(S) Aaron J. Zeigler				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) This thesis explores the complex relationship between automatic license plate reader (ALPR) expansion programs and data privacy. As advanced ALPR systems have become more pervasive in American society, concerns regarding data privacy and civil liberties have surfaced. In discussing various use cases of ALPR technology, from locating stolen vehicles to identifying wanted persons, this thesis explores how law enforcement can expand ALPR surveillance programs while also balancing data privacy demands in a democratic society. Using a comparative analysis, this study assesses best data-storage policy guidelines in the United States and the United Kingdom to derive standardized data retention policies for U.S. law enforcement agencies. This study also examines legal frameworks and the regulatory controls governing ALPR technology. While privacy issues will emerge as American culture prioritizes civil liberties, no matter police departments' use of ALPR technology, if the technology is leveraged responsibly, it will prove to be a powerful surveillance tool in police patrol operations. If American police departments continue to expand ALPR programs, new legislation will be needed to establish national data retention standards, which will ultimately benefit law enforcement by improving transparency and accountability and reducing data storage costs. This study offers several policy recommendations with a forward-looking perspective, anticipating future developments in ALPR technology.				
14. SUBJECT TERMS ALPR, automatic license plate reader, data privacy, surveillance			15. NUMBER OF PAGES 77	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

ALPR EXPANSION PROGRAMS AND DATA PRIVACY

Aaron J. Zeigler
Police Sergeant, Glendale (California) Police Department
BA, San Diego State University, 2003
MPA, California State College at Long Beach, 2008

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2023**

Approved by: David W. Brannan
Co-Advisor

Anshu N. Chatterjee
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis explores the complex relationship between automatic license plate reader (ALPR) expansion programs and data privacy. As advanced ALPR systems have become more pervasive in American society, concerns regarding data privacy and civil liberties have surfaced. In discussing various use cases of ALPR technology, from locating stolen vehicles to identifying wanted persons, this thesis explores how law enforcement can expand ALPR surveillance programs while also balancing data privacy demands in a democratic society. Using a comparative analysis, this study assesses best data-storage policy guidelines in the United States and the United Kingdom to derive standardized data retention policies for U.S. law enforcement agencies. This study also examines legal frameworks and the regulatory controls governing ALPR technology. While privacy issues will emerge as American culture prioritizes civil liberties, no matter police departments' use of ALPR technology, if the technology is leveraged responsibly, it will prove to be a powerful surveillance tool in police patrol operations. If American police departments continue to expand ALPR programs, new legislation will be needed to establish national data retention standards, which will ultimately benefit law enforcement by improving transparency and accountability and reducing data storage costs. This study offers several policy recommendations with a forward-looking perspective, anticipating future developments in ALPR technology.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	AUTOMATED LICENSE PLATE READERS AND DATA PRIVACY: AN INTRODUCTION.....	1
A.	PROBLEM STATEMENT	3
B.	RESEARCH QUESTION	4
C.	LITERATURE REVIEW	4
	1. Law Enforcement and Democracy	5
	2. Law Enforcement and Surveillance	7
	3. Data Privacy and Technology	9
	4. Summary.....	11
D.	RESEARCH DESIGN	12
II.	LAW ENFORCEMENT AND SURVEILLANCE	13
A.	SURVEILLANCE AND PRIVACY RIGHTS	13
B.	DIGITAL RECOGNITION NETWORK	15
C.	ALPR EXPANSION PROGRAMS.....	16
D.	ALGORITHMIC GOVERNANCE AND ALGOCRACY THEORY	18
E.	MOSAIC THEORY AS AN APPLIED FRAMEWORK.....	21
	1. ALPR Privacy.....	22
	2. ALPRs and Civil Liberties	22
	3. ALPR Data Sharing.....	23
	4. Misuse of ALPR Data	23
F.	CONCLUSION	25
III.	DATA PRIVACY	27
A.	VARIABLE DATA RETENTION STANDARDS.....	27
B.	COMPARATIVE ALPR POLICY CASE STUDIES.....	32
C.	DATA SECURITY	37
D.	FUTURE OUTLOOK FOR ALPR EXPANSION PROGRAMS	39
IV.	EXPANDING ALPR PROGRAMS	43
A.	U.S. LAW ENFORCEMENT POLICY RECOMMENDATIONS....	44
	1. Federally Approved Data Retention Period	44
	2. Data Collection	45
	3. Data Access and Sharing.....	45
	4. Data Security	45

5.	Public Engagement and Transparency	46
6.	Oversight and Accountability	46
B.	DISCUSSION FOR FUTURE RESEARCH	46
LIST OF REFERENCES		49
INITIAL DISTRIBUTION LIST		57

LIST OF FIGURES

Figure 1.	Symmetric Cryptography.....	38
-----------	-----------------------------	----

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	California’s ALPR Data Retention and Privacy Laws.	29
Table 2.	Summary of Police Data Retention Periods and Dispositions.....	36

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
AES	Advanced Encryption Standard
ALPR	automated license plate reader
ANPR	automated number plate recognition
CHP	California Highway Patrol
DHS	Department of Homeland Security
DPIA	data privacy impact assessment
DRN	Digital Recognition Network
EFF	Electronic Frontier Foundation
ISS	Investigative Support Section
LPR	license plate reader
MDC	Metropolitan Police Department of the District of Columbia
PD	police department

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis explores the complex relationship between automated license plate reader (ALPR) expansion programs and data privacy. As police departments have scaled up their use of surveillance technology, concerns over data privacy and civil liberties have emerged.¹ This research explores how police departments can deploy ALPR technology at scale while also balancing crime reduction and privacy demands in a democratic society. Various use applications of ALPR systems are discussed, from recovering stolen vehicles to identifying wanted persons.² This study identifies the literary gaps and explores the challenges faced by law enforcement in successfully expanding ALPR programs. Employing a comparative policy analysis approach, this study evaluates optimal data storage practices in both the United States and the United Kingdom, aiming to establish a uniform data retention policy across U.S. law enforcement agencies. Additionally, this study explores the legal frameworks and regulatory constraints that govern ALPR technology.

The research findings reveal that regardless of how rapidly law enforcement adopts ALPR technology, privacy concerns will inevitably emerge, given the significance attached to civil liberties within American culture. However, if leveraged responsibly, ALPR technology can be a powerful tool to enhance police patrol operations.³ New legislation and policy guidelines are needed to address the rapid expansion of ALPR programs in the United States.

This thesis concludes that adopting a national 90-day ALPR data retention policy comes with the inherent advantages of law enforcement's having better data hygiene and

¹ Hannah Bloch-Wehba, "Visible Policing: Technology, Transparency, and Democratic Control," *California Law Review* 109, no. 3 (June 2021): 917–78, <https://www.californialawreview.org/print/visible-policing-technology-transparency-and-democratic-control/>.

² Dave Maass, "Automated License Plate Readers Threaten Abortion Access. Here's How Policymakers Can Mitigate the Risk," Electronic Frontier Foundation, September 28, 2022, <https://www.eff.org/deeplinks/2022/09/automated-license-plate-readers-threaten-abortion-access-heres-how-policymakers>.

³ Cynthia Lum et al., "The Rapid Diffusion of License Plate Readers in US Law Enforcement Agencies," *Policing* 42, no. 3 (2019): 376–93, <https://doi.org/10.1108/PIJPSM-04-2018-0054>.

accountability and being alleviated of the burden of data storage.⁴ Policy recommendations presented in this study contribute to the ongoing conversation about balancing the benefits of ALPR expansion with the imperative of safeguarding individual data privacy. Moreover, this thesis underscores the need for continual policy adjustments and new legislation to address advancements in ALPR technology. As the technology landscape evolves, regular collaboration between policymakers, law enforcement agencies, and community stakeholders will be crucial in shaping policies that strike a balance between effective law enforcement and the fundamental rights of privacy.

By analyzing potential benefits and identifying policy challenges, this thesis offers policy recommendations that address emerging law enforcement trends in ALPR technology that will shape new legislation. This study also contributes to the ongoing public discourse surrounding ALPR expansion programs in democratic societies. Privacy concerns inevitably emerge as personal freedoms are challenged. However, geopolitical pressures and the demands to secure our homeland warrant new ways to keep our communities safe. In summary, this thesis provides a national framework that not only suggests practical policy measures to navigate the evolving landscape of ALPR technology but also adds depth to the conversation about responsible ALPR growth and safeguarding data privacy.

⁴ Joe Littell, Maggie Smith, and Nick Starck, “The Devil Is in the Data: Publicly Available Information and the Risks to Force Protection and Readiness,” Modern War Institute, September 20, 2022, <https://mwi.westpoint.edu/the-devil-is-in-the-data-publicly-available-information-and-the-risks-to-force-protection-and-readiness/>.

ACKNOWLEDGMENTS

First and foremost, I would like to extend my deepest gratitude to my loving wife, Kelly, and our precious daughter, Zoe. Your unconditional support, patience, and encouragement have been the pillars of my strength throughout the challenging journey of this master's program at NPS's Center for Homeland Defense and Security. It is your belief in my abilities and your sacrifices that have been instrumental in shaping my academic success.

I am equally thankful to my esteemed NPS professors and faculty advisors, Dr. David Brannan and Dr. Anshu Chatterjee. Your mentorship, guidance, and unwavering support throughout the writing process have been invaluable. Your dedication to imparting knowledge and the genuine interest you take in your students' growth have not only enhanced my learning experience, but also instilled in me a drive for excellence.

To all of you, I owe a debt of gratitude. Thank you for being beacons of light and helping me achieve this significant milestone in my life.

THIS PAGE INTENTIONALLY LEFT BLANK

I. AUTOMATED LICENSE PLATE READERS AND DATA PRIVACY: AN INTRODUCTION

In a world grappling with the implications of artificial intelligence, advanced technology, and emerging crime trends, the United States faces a challenging and complex opportunity to scale up law enforcement automated license plate reader (ALPR) programs to the national level. As the nation aspires for more security measures and balances homeland security demands against the essential need for privacy, expanding ALPR programs is a natural progression. This research outlines the benefits of ALPR expansion programs, identifies the regulatory barriers, and highlights the ethical decisions the United States must navigate to achieve a safer, more secure society.

Introduced in the United Kingdom in the 1980s, ALPRs ushered in a new era of crime prevention strategies. Cities once grappling with terrorist attacks, capturing fleeing suspects, and recovering stolen vehicles suddenly had a powerful surveillance tool at their disposal to identify and apprehend criminals.¹ ALPRs emerged as silent sentinels affixed to light poles at intersections and attached to police vehicles, relentlessly capturing, and storing massive amounts of license plate data to help police identify suspects in real time. As more ALPRs were integrated into police operations, predictive policing models became a reality, optimizing street patrols to identify terrorists, restore public safety, and make streets safer. As the United States realized the benefits of this technology, American law enforcement agencies answered the call to mobilize and scale up ALPR programs to the national level. Police agencies across the country harnessed the power of ALPR surveillance systems in everything from tracking stolen cars, to conducting traffic enforcement, to locating wanted persons.² Private industry, Vigilant Solutions, for example, capitalized on creating robust ALPR databases and later selling ALPR data for

¹ James J. Willis, Christopher Koper, and Cynthia Lum, “The Adaptation of License-Plate Readers for Investigative Purposes: Police Technology and Innovation Re-invention,” *Justice Quarterly* 35, no. 4 (June 2018): 614–38, <https://doi.org/10.1080/07418825.2017.1329936>.

² Dave Maass, “Automated License Plate Readers Threaten Abortion Access. Here’s How Policymakers Can Mitigate the Risk,” Electronic Frontier Foundation, September 28, 2022, <https://www.eff.org/deeplinks/2022/09/automated-license-plate-readers-threaten-abortion-access-heres-how-policy-makers>.

profit.³ Thus, the rise in the surveillance capital industry created controversy in how data are securely stored and protected in both public and private domains.

Subsequently, the path to expanding ALPR programs faced many obstacles. Accelerated ALPR technology adoption, compounded by rising infrastructure costs, the need to train law enforcement personnel, and the complexity of integrating ALPRs into existing surveillance databases, has presented significant hurdles. Perhaps the most significant legal challenges have been outlined in the mosaic theory, which restricts prolonged geo-surveillance by law enforcement.⁴ Meanwhile, growing concerns about data privacy rights in the United States persist.

In a society deeply committed to individual freedoms, the question of how to responsibly scale up ALPR programs without infringing upon civil liberties remains a central concern. The United Kingdom's 2018 Data Privacy Act implemented thoughtful and comprehensive privacy guidelines.⁵ The data retention policies introduced in this statute required that information not linked to active criminal investigation be quickly erased. Data privacy impact assessments and ALPR access restrictions have become the norm, with robust authentication processes to secure and keep the data out of the wrong hands. Transparency and accountability have taken center stage, with more policy restrictions on law enforcement agencies. Increased oversight requires better data hygiene including routine ALPR data purges that regularly disclose how such data are being used. These data privacy measures serve as a social contract, a pact between those who serve and protect and the citizens they watch over.

Expanding ALPR programs in the United States remains a complicated yet necessary national security endeavor. Uniform ALPR data retention standards and regular

³ Jared Kirby, "Federal Judge Rules in Favor of Digital Recognition Network (DRN) in Antitrust Case," DRN, November 9, 2018, <https://drndata.com/news/federal-judge-rules-favor-digital-recognition-network-drn-antitrust-case/>.

⁴ Monu Bedi, "Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory," *Boston University Law Review* 94, no. 6 (December 2014): 1809–80, <https://www.bu.edu/bulawreview/files/2014/12/BEDI.pdf>.

⁵ David Gilmartin and Kerry Childe, "Developing a Data Retention Policy That Meets Privacy Requirements," ACC Docket, January 2, 2023, <https://docket.acc.com/developing-data-retention-policy-meets-privacy-requirements>.

data audits to ensure compliance with data privacy laws are essential components of a national policy framework. Police departments in the United States must continue to carefully navigate a future where public safety and privacy demands seamlessly coalesce. By forging strategic partnerships with privacy advocates, engaging community stakeholders early in the process, and prioritizing data privacy, police departments can responsibly expand ALPR programs in the United States.

A. PROBLEM STATEMENT

Public and private uses for ALPR technology spark a growing tension between privacy advocates and the government due to the technology's expansion into public and private spaces. Police ALPR surveillance cameras amass significantly more vehicle images than any individual police officer might collect, and these license plate images are stored within databases that enable investigators to scrutinize them later for more complex and advanced queries into major criminal cases.⁶ Police departments throughout the country deploy ALPR technology systems with advanced high-resolution cameras. The latter alerts officers about actionable information and provides high-resolution photos of vehicles. Most of the debate concerns data security and third-party information sharing. ALPR technology provides location data, and its sale to non-government actors for commercial use can be profitable.⁷

There is no doubt that ALPR technology has been helpful in reducing crime. Police officers have solved crimes and conducted more efficient criminal investigations through regional ALPR data-sharing networks.⁸ ALPR cameras have recovered stolen vehicles and identified vehicles used in crimes. ALPRs also have the added benefit of providing law enforcement with greater access to information.

⁶ Cynthia Lum et al., "The Rapid Diffusion of License Plate Readers in US Law Enforcement Agencies," *Policing* 42, no. 3 (2019): 376–93, <https://doi.org/10.1108/PIJPSM-04-2018-0054>.

⁷ Kate Kaye, "Private Dollars Are Seeding Surveillance Tech across the US," Smart Cities Dive, February 5, 2021, <https://www.smartcitiesdive.com/news/private-dollars-are-seeding-surveillance-tech-across-the-us/594615/>.

⁸ Louise Matskis, "Can License Plate Readers Really Reduce Crime?," *Wired*, October 24, 2019, <https://www.wired.com/story/flock-safety-license-plate-readers-crime/>.

The private sector has also quietly expanded its camera networks through retail businesses and homeowners' associations and joined regional data-sharing networks, which have optimized ALPR cameras' machine-learning capabilities. The commercialization of ALPRs has allowed police departments to rapidly expand these programs and request unrestricted access to privately owned cameras. This coverage has created robust ALPR data repositories for police to conduct criminal investigations. The added benefit of ALPR camera searches in police investigations has demonstrated widespread utility and positively reduced crime.⁹

Yet, expanded access to ALPR data has recently encountered sharp criticism and presented unresolved legal challenges in the courts. Privacy advocates have raised objections against law enforcement's ability to access ALPR databases to enforce criminal laws. This limitation has removed a valuable crime reduction tool because restricting access to ALPR data eliminates a valuable investigatory resource to deter crime and apprehend criminals. Stronger federal and state regulations on ALPR data create legal barriers for police to gather and collect evidence to solve crimes.

B. RESEARCH QUESTION

How can police departments deploy ALPR technology at scale while also balancing crime reduction and data privacy demands in a democratic society?

C. LITERATURE REVIEW

Considering police reforms and calls for greater transparency, police departments have sought an equilibrium between expanding surveillance camera programs and observing privacy laws.¹⁰ ALPR programs have reenergized new debates on the appropriate balance between police surveillance and privacy rights. Growing tension has

⁹ Ian Warren et al., "When the Profile Becomes the Population: Examining Privacy Governance and Road Traffic Surveillance in Canada and Australia," *Current Issues in Criminal Justice* 25, no. 2 (November 2013): 565–84, <https://doi.org/10.1080/10345329.2013.12035984>.

¹⁰ Yash Dattani, "Big Brother Is Scanning: The Widespread Implementation of ALPR Technology in America's Police Forces," *Vanderbilt Journal of Entertainment and Technology Law* 24, no. 4 (2022): 749–85, <https://scholarship.law.vanderbilt.edu/jetlaw/vol24/iss4/3>.

arisen over the increasing use of surveillance cameras by law enforcement. Police officers regularly face challenges to ensuring citizens' safety while preserving their civil liberties.

This research illuminates how police departments can successfully expand ALPR programs in the United States and where the tension between police trust and civilian expectations around data privacy remains in the spotlight. This literature review examines these debates, highlighting existing research and identifying gaps to advance these concerns. The literature review here explores issues associated with the police and ALPR surveillance programs in a democratic society. Understanding how variable ALPR data retention standards affect privacy is also essential. Extensive scholarly research addresses data privacy and police mistrust.¹¹

1. Law Enforcement and Democracy

Police officers have endured widespread civil unrest in recent years, and the need to define their role in society is more pronounced than ever. Law enforcement in democratic countries ensures the protection of individual rights, and the police enforce laws implemented by the federal, state, and local governments that represent the people.¹² The police's role is contentious because police departments must constantly justify their actions, which often intrude into citizens' private spaces. Several scholars have written about law enforcement's role, and much of the academic debate is rooted in police legitimacy and calls for greater transparency.¹³ Police officers are accountable to their communities, and severe punishment must follow any police misconduct. Law enforcement's duty to protect and serve civilians will continually clash with increased societal expectations of personal privacy, a topic that persists with ALPR technologies and data privacy. This dilemma can lead to greater police mistrust as private-sector messaging reinforces the societal need for data protection while law enforcement focuses on public safety over personal privacy.

¹¹ Dattani.

¹² Dattani.

¹³ Dattani.

Law enforcement officers negotiate the demands and expectations of several government entities. According to Stone and Ward, federal and state agencies, including the executive, legislative, and judicial branches, hold police departments accountable.¹⁴ Increased crime and pervasive violence in urban communities compel some citizens to accept more restrictions on their freedoms by the police—even though these groups have limited discretion over the police surveillance strategies implemented in their residential communities.¹⁵ Sankar Sen advocates implementing civilian-led oversight commissions to provide greater accountability. These commissions review police misconduct and impose recommendations to assist with police reform.¹⁶ The aim of citizen review boards is to remove any negative sentiment surrounding discriminatory or unfair policing practices.

Still, law enforcement officials and civic leaders increasingly disagree on the degree of civilian oversight. Federally mandated consent decrees impose policy reforms when the federal government discovers a pattern of police misconduct or civil rights violations.¹⁷ In democratic societies, these mutual agreements between federal, state, and local police departments aim to provide greater transparency and expand community oversight. According to Alpert, McLean, and Wolfe, consent decrees experience short-term success but are challenging to sustain.¹⁸ Report findings from consent decrees are usually confidential and do not require police reforms after meeting mandate requirements. Alpert, McLean, and Wolfe’s study reveals that policy recommendations often stall after funds to support police reform disappear.¹⁹ Thus, policy recommendations are fleeting and lack impact.

¹⁴ Christopher E. Stone and Heather H. Ward, “Democratic Policing: A Framework for Action,” *Policing and Society* 10, no. 1 (2000): 11–45, <https://doi.org/10.1080/10439463.2000.9964829>.

¹⁵ Stone and Ward.

¹⁶ Sankar Sen, *Enforcing Police Accountability through Civilian Oversight* (New Delhi: SAGE Publications, 2010).

¹⁷ Christopher Stone, Todd Foglesong, and Christine M. Cole, *Policing Los Angeles under a Consent Decree: The Dynamics of Change at the LAPD* (Cambridge, MA: Harvard Kennedy School, 2009), <https://www.hks.harvard.edu/publications/policing-los-angeles-under-consent-decree-dynamics-change-lapd>.

¹⁸ Geoffrey P. Alpert, Kyle McLean, and Scott Wolfe, “Consent Decrees: An Approach to Police Accountability and Reform,” *Police Quarterly* 20, no. 3 (2017): 239–49, <https://doi.org/10.1177/1098611117709591>.

¹⁹ Alpert, McLean, and Wolfe.

The need to enforce laws and protect civil liberties in a democratic society is a delicate balance. As more police professionals deploy ALPR camera systems, ALPR expansion programs confirm the need for more surveillance cameras to assist police with criminal investigations. Despite their success, ALPR cameras have also been the source of vigorous debate among the American Civil Liberties Union (ACLU) and legal scholars. The District of Columbia Court introduced the mosaic theory as a legal framework to acquit a defendant after a month-long warrantless GPS surveillance operation.²⁰ This decision created a legal roadblock and stifled law enforcement's ability to use geo-surveillance in criminal investigations.

2. Law Enforcement and Surveillance

Police officers' strategic use of ALPR surveillance cameras is an invaluable investigative tool yet sparks debate on the acceptable levels of surveillance in a democracy. Watchdog organizations like the ACLU and the Electronic Frontier Foundation (EFF) closely monitor law enforcement overreach and vigorously advocate greater regulatory control to safeguard citizens from unreasonable privacy violations. Friedman et al., proponents of judicial governance of police technology, assert police surveillance cameras are force multipliers that infringe upon citizens' privacy.²¹ However, more significant restrictions on ALPR use will help criminals avoid detection. According to Wesner and Blevins, police officers who rely on ALPR data eliminate racial bias and the risk of making poor judgments.²² Often, motorists' identities are unknown because ALPRs leverage computer vision and machine learning to scan millions of license plates. In this way, police officers remain neutral and rely on ALPR cameras to develop investigative leads.

Another important debate about police surveillance programs emerged after the courts introduced mosaic theory as a legal theory to safeguard privacy. Schlabach lauds the

²⁰ Bedi, "Social Networks, Government Surveillance."

²¹ Barry Friedman et al., "Policing Police Tech: A Soft Law Solution," *Berkeley Technology Law Journal* 37, no. 2 (2022): 701–756, <https://lawcat.berkeley.edu/record/1257876>.

²² Kearston Wesner and Katie Blevins, "Restraining the Surveillance Society: Comparing Privacy Policies for Automated License Plate Readers in the United States and the United Kingdom," *Ohio State Technology Law Journal* 18, no. 1 (2021): 99–156, <http://hdl.handle.net/1811/101513>.

merits of the mosaic approach in providing further legal protections for private citizens moving in public spaces.²³ The DC Circuit court applied the mosaic theory as a legal framework to acquit a defendant.²⁴ Thus, law enforcement's ability to access ALPR data to conduct geolocation surveillance has become more restricted.

Police surveillance traditionally refers to the monitoring, tracking, and collecting of information by law enforcement agencies to reduce crime. This activity can include various techniques, such as surveillance cameras, wiretapping, and GPS tracking. Advanced technologies like ALPR camera systems can be integrated into police surveillance programs. Police can use ALPR surveillance cameras for crime prevention and community safety. However, ALPRs can also raise concerns about privacy and civil liberties, as well as bias and discrimination.²⁵ Some critics argue that ALPRs disproportionately target marginalized communities and increase racial profiling.²⁶ A debate rages on about the appropriate oversight and transparency of such police surveillance activities.

Recovering stolen vehicles and finding wanted persons are only a few of the wide applications of ALPR technology. ALPR expansion programs have improved case closure rates, based on a 2019 study by Koper and Lum.²⁷ Capitalizing on Department of Homeland Security (DHS) grant funds, some police departments have deployed ALPR cameras to optimize criminal investigations and apprehend criminals. Yet, some scholars argue ALPR expansion programs extend beyond criminal investigations and lead to mundane passive surveillance. Pereira and Raetzsch assert that commonplace ALPR

²³ Gabriel R. Schlabach, "Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act," *Stanford Law Review* 67, no. 3 (March 2015): 677–721, <https://www.jstor.org/stable/43920972>.

²⁴ Schlabach.

²⁵ Jason Kelley and Matthew Guariglia, "Things to Know before Your Neighborhood Installs an Automated License Plate Reader," Electronic Frontier Foundation, September 14, 2020, <https://www.eff.org/deeplinks/2020/09/flock-license-plate-reader-homeowners-association-safe-problems>.

²⁶ Dave Maass and Hayley Tsukayama, "EFF Joins Effort to Restrict Automated License Plate Readers in California," Electronic Frontier Foundation, March 19, 2021, <https://www.eff.org/deeplinks/2021/01/eff-joins-effort-restrict-automated-license-plate-readers-california>.

²⁷ Christopher S. Koper and Cynthia Lum, "The Impacts of Large-Scale License Plate Reader Deployment on Criminal Investigations," *Police Quarterly* 22, no. 3 (2019): 305–29, <https://doi.org/10.1177/1098611119828039>.

programs create a complex system of interconnected surveillance networks that go uncontested because of a lack of public understanding.²⁸ Brayne maintains that the character of ALPRs allows police to review massive amounts of stored license plate data to assist with criminal investigations.²⁹ However, Merola, Lum, and Murphy warn that such ALPR surveillance programs could harm the public's perception of the police as these systems store and analyze data even while citizens are under no criminal suspicion.³⁰ The emergence of a closely monitored and surveilled society undermines American democratic norms, whereby individuals enjoy civil liberties free from government oversight. More focused research is needed to explore how deeply embedded ALPR camera infrastructure interacts with less-visible computer-enabled algorithmic structures.³¹ The act of ALPRs' passively collecting license plates and storing them into databases eventually leads to the community's acceptance of banal surveillance.³² ALPR systems cast a wide surveillance net, raising concerns about whether such technology can ensure citizens' data privacy.

3. Data Privacy and Technology

Scholars diverge widely on data privacy. The variances in data retention standards have stimulated vigorous debate in recent years about how long ALPR data should remain in police databases. In the absence of federal guidelines on data retention, police departments defer to their own policies. Lum et al. affirm that law enforcement experts are still uncertain about the best data storage practices.³³ Warren et al. highlight the vast differences among states' data retention standards—from Maine (21 days) to New Jersey

²⁸ Gabriel Pereira and Christoph Raetzsch, "From Banal Surveillance to Function Creep: Automated License Plate Recognition (ALPR) in Denmark," *Surveillance & Society* 20, no. 3 (2022): 265–80, <https://doi.org/10.24908/ss.v20i3.15000>.

²⁹ Sarah Brayne, "Big Data Surveillance: The Case of Policing," *American Sociological Review* 82, no. 5 (2017): 977–1008, <https://doi.org/10.1177/0003122417725865>.

³⁰ Linda M. Merola, Cynthia Lum, and Ryan P. Murphy, "The Impact of License Plate Recognition Technology (LPR) on Trust in Law Enforcement: A Survey-Experiment," *Journal of Experimental Criminology* 15, no. 1 (March 2019): 55–66, <https://doi.org/10.1007/s11292-018-9332-8>.

³¹ Pereira and Raetzsch, "From Banal Surveillance to Function Creep."

³² Pereira and Raetzsch.

³³ Lum et al., "The Rapid Diffusion of License Plate Readers."

(five years).³⁴ Inconsistent data retention standards ultimately hinder law enforcement from using that information for legitimate police investigations.

These discrepancies in data retention laws allow the ALPR industry to go unregulated. Using technology in data collection and analysis spurs debate over better data hygiene and stronger constitutional protections. However, a lack of clear guidelines from the judicial system makes it difficult to determine the appropriate use of this technology and ensure the protection of individual rights. A lack of judicial clarity has stalled the debate over whether the use of this technology should promote better data hygiene and implicates the need for greater constitutional protections.³⁵ Disagreement among scholars over citizens' data privacy persists.

ALPR programs rapidly expanded in the public and private sectors. According to Dattani, ALPR technology has been widely deployed in the United States and requires more regulatory controls.³⁶ Munn argues that expanding ALPR networks into residential neighborhoods, community centers, and urban areas presents data collection opportunities that can capture personal images beyond license plates.³⁷ However, the variances in data storage allow citizens' information to remain in databases for extended periods.³⁸ Therefore, protecting citizens' privacy is essential to avoid unnecessary data breaches.

Private corporations like Vigilant Solutions profit from deregulation, having created large ALPR data repositories. Law enforcement partnerships with third-party ALPR data brokers have shaped the debate about who owns the stored data.³⁹ Kaye argues that as more surveillance technology evolves in the private sector and uses proprietary algorithms, companies effectively avoid state restrictions that city governments impose on

³⁴ Warren et al., "When the Profile Becomes the Population."

³⁵ Dattani, "Big Brother Is Scanning."

³⁶ Dattani.

³⁷ Luke Munn, "Staying at the Edge of Privacy: Edge Computing and Impersonal Extraction," *Media and Communication* 8, no. 2 (2020): 270–79, <https://doi.org/10.17645/mac.v8i2.2761>.

³⁸ Dattani, "Big Brother Is Scanning."

³⁹ David Horrigan, "Data Privacy vs. Crime Prevention: The Automated License Plate Recognition Debate," American Bar Association, August 23, 2021, https://www.americanbar.org/groups/tort_trial_insurance_practice/committees/automobile-litigation/data-privacy-vs-crime-prevention/.

their employees.⁴⁰ Additionally, Dattani contends, “Government and private sector investments have led to rapid advancements in ALPR scanners and databases, turning this once-remedial technology limited to border security into a powerful technology being implemented into police forces nationwide.”⁴¹ Corporate profits accelerate ALPR expansion programs as the private sector benefits from reselling customer geolocation data to third parties.

Underlying all these issues is the deep mistrust of police departments. According to Hofer, due to the extensive scope and depth of data collected by ALPR networks, law enforcement officials anticipate that malicious individuals will aim to compromise sensitive information stored in ALPR databases.⁴² The potential for data breaches only increases as more ALPR networks link regionally, undermining police efforts to secure data because each region collects and stores data autonomously. These interdependent systems create large data repositories that optimize data-sharing networks; however, ensuring individual data privacy is more difficult with such a system.

4. Summary

This literature review articulated the benefits of expanding ALPR surveillance programs, identified issues, and explored the unintended consequences of mass ALPR surveillance programs for citizens. This research adds to the debate and discussions surrounding potential solutions by exploring how police departments have successfully expanded ALPR programs in a climate of police mistrust with increased demand for data privacy. More research must illuminate how police should balance the need to conduct law enforcement investigations with the civilian mandate for ensuring data privacy.

⁴⁰ Kate Kaye, “Setting Guardrails,” February 8, 2021, in *City Surveillance Watch*, produced by Smart Cities Dive, podcast, MP3 audio, 58:20, <https://www.smartcitiesdive.com/news/city-surveillance-watch-setting-guardrails/594495/>.

⁴¹ Dattani, “Big Brother Is Scanning,” 752.

⁴² Jonathan Hofer, “The Pitfalls of Law Enforcement License Plate Readers in California and Safeguards to Protect the Public,” Independent Institute, August 16, 2022, <https://www.independent.org/publications/article.asp?id=14254>.

D. RESEARCH DESIGN

This research demanded an understanding of current ALPR applications before I could investigate their advantages and possible concerns. I employed a policy analysis framework to review police departments' policies, examine the challenges police administrators face in scaling ALPR programs, and identify potential concerns for future deployment. Through the analysis, which followed a comparative case study methodology, I identified multiple cases of ALPR use.

The research process involved collecting and organizing data to identify patterns and trends in ALPR usage and evaluating the effectiveness of existing policies and guidelines to protect citizens' privacy and civil liberties. Then, I reviewed current literature and researched the impact of ALPR use on data privacy and civil rights. I compared existing U.S. and UK policy guidelines from various journal articles, peer-reviewed publications, and open-source government documents in the public domain.

Next, I explored data on ALPR usage, including information on the agencies using such systems and the data they collect and store. Such a step required ethical considerations because any use of private data would have implications for the research and require that I follow ethical guidelines. Although I had several informal discussions with police administrators, I limited my analysis to publicly accessible data found in the public domain that were published by the respective law enforcement organizations.

II. LAW ENFORCEMENT AND SURVEILLANCE

Law enforcement and surveillance are closely related in that law enforcement agencies depend on the latter to support criminal investigations and prosecutions. Surveillance can take many forms, including direct and passive surveillance, and the American perspective on public surveillance is often at odds with what is tolerated by other nations, including mature liberal democracies. The relationship between law enforcement and surveillance is an important issue of constitutional importance. The triangular relationship between the constitution, police, and community also informs the important nexus between law enforcement surveillance and the level of legitimacy police enjoy from the communities they patrol. This chapter explores how the expansion of ALPR surveillance programs impacts personal privacy rights in public spaces. More importantly, it reveals how incredibly useful ALPR technology is for law enforcement, but its use needs to balance citizens' privacy demands.

A. SURVEILLANCE AND PRIVACY RIGHTS

As surveillance technology, ALPRs help law enforcement automatically capture images of license plates and convert them into digital data that can be used to track and monitor vehicle movements. ALPRs are a profitable business proposition, according to a recent study, growing from a \$794.1 million global market in 2019 to a projected \$1.2 billion by 2025.⁴³ Law enforcement agencies increasingly rely on both passive and active surveillance methods to carry out their duties effectively. Police departments have doubled their efforts and expanded police surveillance programs from additional federal and state funding sources.⁴⁴ Passive surveillance involves the use of technologies such as ALPR systems to monitor traffic patterns, enforce traffic violations, and recover stolen vehicles.⁴⁵

⁴³ Horrigan, "Data Privacy vs. Crime Prevention."

⁴⁴ Lum et al., "The Rapid Diffusion of License Plate Readers."

⁴⁵ Ajay Prasad, Kaushik Ghosh, and Sourabh Singh Verma, "Crime Patrolling Assistance Using Passive Monitoring: A Proof of Concept of a Proactive Wi-Fi Surveillance System," in *Proceedings of the 12th International Conference on Computing Communication and Networking Technologies* (Piscataway, NJ: IEEE, 2021), 1–11, <https://doi.org/10.1109/ICCCNT51525.2021.9579805>.

Conversely, active surveillance focuses on criminal investigations related to drug enforcement, homicide cases, and suspect and fugitive pursuits for other serious crimes. ALPR technology entails passive surveillance in that it captures the license plate of every vehicle that comes into the camera's view.

In terms of scaling up police ALPR programs, significant advancements in surveillance technology and the use of such technology have greatly expanded in the public and private domains. The scale of usage has raised questions about how best to regulate and control ALPR technology.⁴⁶ Privately owned networks like Motorola Solutions have capitalized on the highly lucrative, unregulated license plate collection industry.⁴⁷ Motorola Solutions sells ALPR data to auto repossessioners through its commercial division, Digital Recognition Network (DRN). In addition to government agencies, DRN primarily markets its ALPR database to car rental companies, auto loan lenders, repo-collection agencies, and insurance agencies.⁴⁸ Thus, the use of these programs in the private sector is more intrusive because companies commoditize consumer profiles that are later sold for profit.

Additional funding from public and private sources subsidizes ALPR programs. Specifically, DHS's homeland security grants have accelerated the expansion of ALPR programs in the public sector.⁴⁹ ALPR technology offers a range of benefits for both public and private sectors with broad commercial applications and reduced hardware costs.⁵⁰ Some private companies rent or loan ALPR equipment to under-resourced police departments to accelerate technology adoption rates and expand ALPR databases. These positive outcomes have also appealed to private donors like Motorola Solutions, Amazon,

⁴⁶ Dan Calacci, Jeffrey J. Shen, and Alex Pentland, "The Cop in Your Neighbor's Doorbell: Amazon Ring and the Spread of Participatory Mass Surveillance," *Proceedings of the ACM on Human-Computer Interaction* 6, no. CSCW2 (November 2022): 1–47, <https://doi.org/10.1145/3555125>.

⁴⁷ Nicole K. McConlogue, "Discrimination on Wheels: How Big Data Uses License Plate Surveillance to Put the Brakes on Disadvantaged Drivers," *Stanford Journal of Civil Rights & Civil Liberties* 18 (2022): 269–332, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839726.

⁴⁸ McConlogue.

⁴⁹ Julia M. Brooks, "Drawing the Lines: Regulation of Automatic License Plate Readers in Virginia," *Richmond Journal of Law and Technology* 25, no. 3 (2019): 1–32, <https://jolt.richmond.edu/drawing-the-lines-regulation-of-automatic-license-plate-readers-in-virginia/>.

⁵⁰ Dattani, "Big Brother Is Scanning."

and Microsoft, which have further expanded police ALPR programs around the country.⁵¹ Private equity in the form of seed money has helped fund police foundations around the country to improve community safety and grow ALPR programs.⁵² Private enterprise is advocating and funding the expansion of ALPR programs by law enforcement.

B. DIGITAL RECOGNITION NETWORK

Privately owned surveillance networks like DRN capture millions of vehicle license plates, log their geolocation data, and track vehicle movement.⁵³ The company primarily markets its database to car rental companies, auto loan lenders, repo-collection agencies, and insurance agencies. Additionally, private investigators and other non-government actors are willing to pay premiums for access to DRN's database.⁵⁴ Thus, DRN acts as a large data repository that collects its own information as well as ALPR data contributed by law enforcement.⁵⁵

DRN uses a fleet of unmarked vehicles equipped with high-speed cameras that capture millions of license plate images and crowdsources that information in its database.⁵⁶ Vehicle recovery agents are financially incentivized to install DRN cameras on their vehicles, scan license plates, and then upload the data to DRN during their regular work shifts.⁵⁷ After the data are uploaded, DRN analyzes the information and uses software to predict where certain vehicles may travel. Depending on location data, DRN can build a full story of a vehicle owner's driving patterns.

⁵¹ Kaye, "Private Dollars Are Seeding Surveillance Tech across the US."

⁵² Kaye.

⁵³ McConlogue, "Discrimination on Wheels."

⁵⁴ Thor Benson, "The Danger of License Plate Readers in Post-Roe America," *Wired*, July 7, 2022, <https://www.wired.com/story/license-plate-reader-alpr-surveillance-abortion/>.

⁵⁵ Kirby, "Federal Judge Rules in Favor of DRN."

⁵⁶ Randy L. Dryer and S. Shane Stroud, "Automatic License Plate Readers: An Effective Law Enforcement Tool or Big Brother's Latest Instrument of Mass Surveillance? Some Suggestions for Legislative Action," *Jurimetrics* 55, no. 2 (Winter 2015): 225–74, <https://www.jstor.org/stable/24395572>.

⁵⁷ "Street-Level Surveillance: Automated License Plate Readers (ALPRs)," Electronic Frontier Foundation, accessed September 6, 2023, <https://www.eff.org/pages/automated-license-plate-readers-alpr>.

DRN's data collection methods are inconspicuous as motorists drive around heavily populated residential neighborhoods and shopping centers. Recently, DRN faced a lawsuit that alleged its proprietary algorithm was intrusive and had violated privacy laws.⁵⁸ Specifically, DRN's "vehicle stories" retain sensitive geolocation and temporal data for unsuspecting motorists who are unaware they are under surveillance. Third parties may purchase these stories to infer motorists' political affiliations, medical histories (e.g., visiting abortion clinics or cancer treatment centers), dating preferences, social clubs, and dining habits.⁵⁹ DRN generates these stories without the subjects' being under criminal investigation or being placed on a watch list and without their knowledge of governmental or private surveillance. Consumer ALPR data are incorporated within proprietary analytical tools to assess risk and credit worthiness for auto lenders.⁶⁰ DRNsights Analytics provides auto financiers with data to locate vehicle assets and confirm recovery of vehicles in the case of loan defaults.⁶¹ Harvesting ALPR data is essential for surveillance expansion programs because it provides predictive analytics that generates consumer profiles based on driving patterns while supplying law enforcement with useful data for criminal prosecution. The private sector collects ALPR data on a massive scale with minimal restraints on its use. Thus, it is prudent to analyze the benefits and limitations of expanding ALPR programs in law enforcement.

C. ALPR EXPANSION PROGRAMS

Scaling up law enforcement ALPR programs is a natural progression toward optimizing police surveillance. Major technological advances have created more opportunities for police departments to network, link, and scale up surveillance programs through modern ALPR infrastructure.⁶² High-resolution ALPR cameras capture more vehicle images than police officers patrolling a district. Large capital investments in smarter technologies that reduce crime, enforce laws, and improve city governance are an

⁵⁸ Kirby, "Federal Judge Rules in Favor of DRN."

⁵⁹ Maass, "Automated License Plate Readers Threaten Abortion Access."

⁶⁰ McConlogue, "Discrimination on Wheels."

⁶¹ McConlogue.

⁶² Pereira and Raetzsch, "From Banal Surveillance to Function Creep."

emerging trend in the urban landscape.⁶³ Law enforcement relies heavily on automated technology developed by public and private partnerships to meet public safety demands. For example, private companies manufacture and develop police body cameras, ALPRs, and facial recognition technology for law enforcement to deploy. Thus, police departments must rely solely on private-sector actors that have total control over their proprietary technology, software updates, and corporate policies while law enforcement is treated like any other customer. This trend is likely to continue as artificial intelligence expands into more disciplines and fields, including every aspect of law enforcement.⁶⁴

The convergence of public and private surveillance technologies further complicates privacy claims against law enforcement. Dually purposed and publicly owned, ALPR cameras collect suspicious vehicle license plate images associated with criminal activity while privately owned cameras track and locate delinquent borrowers risking default.⁶⁵ More ALPR cameras are clustered in low-income neighborhoods, with the idea that borrowers will likely default on auto loans in poorer communities. Nevertheless, private corporations that recognize police departments like any other consumers market surveillance technology to law enforcement for their own profit.⁶⁶ The same laws that govern police departments do not hold private corporations accountable or require them to develop new products with the Fourth Amendment in mind. While police forces greatly benefit from ALPR technology, they continually explore responsible methods of deploying ALPR cameras while observing citizens' Fourth Amendment rights.

Increased corporate partnerships and an overreliance on privately developed technology have introduced new legal complexity, which includes merging law enforcement and private data sources in smarter cities. The concept of a smart city

⁶³ Elizabeth E. Joh, "Policing the Smart City," *International Journal of Law in Context* 15 (2019): 177–82, <https://doi.org/10.1017/S1744552319000107>.

⁶⁴ Christopher Rigano, *Using Artificial Intelligence to Address Criminal Justice Needs* (Washington, DC: National Institute of Justice, 2018), <https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs>.

⁶⁵ Joh, "Policing the Smart City."

⁶⁶ Joh, "Policing the Smart City"; Nicoletta Boldrini, "Algocracy and Surveillance Capitalism: We Live in a World Governed by Algorithms," *Medium* (blog), May 30, 2017, <https://nicboldrini.medium.com/algocracy-and-surveillance-capitalism-we-live-in-a-world-governed-by-algorithms-abd1f158186a>.

envision a future where urban life is governed by interconnected sensors, artificial intelligence, and ALPRs integrated into the city's framework.⁶⁷ Such constant data gathering and evaluation promise to optimize pedestrian and vehicle traffic, as well as improve weather readiness and energy consumption. Such mergers facilitate the seamless integration of city services into urban communities. From traffic safety to environmental management, predictive analytics impacts crime prevention decisions, and these advancements greatly improve one's quality of life at the expense of personal privacy.⁶⁸

The expanding role of private entities in policing, as in many other aspects of smart city operations, creates potential pitfalls. The technology used in these scenarios is typically proprietary and often protected by intellectual property laws, potentially limiting transparency and oversight of its use. This limitation can create challenges in maintaining public oversight, preserving individual rights, and ensuring justice and accountability in law enforcement.⁶⁹ For instance, a private company developing predictive policing algorithms may be reluctant to share proprietary software information.⁷⁰ Thus, proprietary algorithms challenge the judicial system's ability to assess privacy claims derived from smart technologies, thereby potentially violating the rights of criminal defendants.

D. ALGORITHMIC GOVERNANCE AND ALGOCRACY THEORY

With the linkage of more ALPR networks and connections to regional networks, traditional policing will become more integrated with technology and less visible to the public.⁷¹ Algocracy theory, which studies the rule of governance by algorithmic structures, can be applied to ALPR systems.⁷² With the installations of more ALPR cameras come more connections with broader regional networks.⁷³ The algorithmic decision-making and

⁶⁷ Joh, "Policing the Smart City."

⁶⁸ Joh.

⁶⁹ Joh.

⁷⁰ Boldrini, "Algocracy and Surveillance Capitalism."

⁷¹ Joh, "Policing the Smart City."

⁷² Boldrini, "Algocracy and Surveillance Capitalism."

⁷³ Maass, "Automated License Plate Readers Threaten Abortion Access."

machine-learning systems of ALPRs are crucial for analyzing large data sets.⁷⁴ ALPR network systems have emerged as powerful investigative tools with advanced algorithms quickly digesting massive amounts of data. Pereira and Raetzsch delineate the roles of the camera and algorithms in ALPR systems:

It is important to distinguish between the *capture* of images by cameras and the different algorithms used for the *recognition* of license plates. . . . ALPR systems require [optical character recognition] algorithms to transform captured images into machine-readable data points [original emphasis]. Algorithms are first employed for different microtasks such as number plate extraction (from the larger image), character segmentation, and character recognition. The recognition of alphanumeric characters most often uses a rule-based algorithm, the most computationally efficient method.⁷⁵

More advanced systems may incorporate machine-learning algorithms concentrated on large-scale data sets.⁷⁶ Therefore, as law enforcement becomes more reliant on ALPR algorithms, it must focus more attentively on the fundamental development of them to avoid biased data sets.

As ALPR programs have expanded nationally, they have optimized police patrols and improved field operations through surveillance cameras. Established ALPR infrastructure represents a tangible illustration of surveillance technology in the community, normalizing the concept of algorithmic vision and automated decision-making.⁷⁷ Within this context, ALPR expansion programs show practitioners how algorithmic decision-making can influence the police. According to Waldman and Martin's study, the perceived legitimacy of governance greatly improves, particularly in critical areas like parole hearings, police patrols, and healthcare, when human-in-the-loop models are incorporated into decision-making processes.⁷⁸ It is, therefore, pragmatic and valuable

⁷⁴ Pereira and Raetzsch, "From Banal Surveillance to Function Creep."

⁷⁵ Pereira and Raetzsch, 269.

⁷⁶ Pereira and Raetzsch.

⁷⁷ Pereira and Raetzsch.

⁷⁸ Ari Waldman and Kirsten Martin, "Governing Algorithmic Decisions: The Role of Decision Importance and Governance on Perceived Legitimacy of Algorithmic Decisions," *Big Data & Society* 9, no. 1 (January 2022): 1–16, <https://doi.org/10.1177/20539517221100449>.

to consider the ethical implications of automated decisions as ALPR expansion programs proliferate.

Ethical decision-making is critical in the discussion of ALPR program scaling. In today's world, technology, particularly algorithms, can significantly influence society, economy, and politics.⁷⁹ Algorithms are pervasive and deeply integrated in post-industrial society: they influence electoral processes, criminal justice systems, and social media feeds.⁸⁰ However, entrusting critical decisions to machines can reveal profound ethical dilemmas related to responsibility, transparency, personal freedom, fairness, and the principles of democracy.⁸¹ In their book, Rubel, Castro, and Pham explain that safety guardrails in algorithmic systems are necessary to ensure citizens fully participate in the political process and prevent algorithms from undermining democracy.⁸² Regular training and human involvement in decision-making processes are important aspects of algorithmic systems. Without safeguards, there is a genuine risk of algorithms eroding democratic values.⁸³ For example, if ALPR machines rely on biased data, they may disproportionately impact minority communities.⁸⁴ Algorithmic bias was at work in 2018, when the Oakland Police Department detained two individuals at gunpoint after their vehicle was incorrectly flagged as stolen.⁸⁵ Indeed, densely populated metropolitan communities tend to have more ALPR cameras installed.⁸⁶ An overreliance on biased ALPR data can also harm community relations and erode public trust, thus reinforcing the need for police officers to always verify ALPR data before taking enforcement action.

⁷⁹ Boldrini, "Algocracy and Surveillance Capitalism."

⁸⁰ Alan Rubel, Clinton Castro, and Adam Pham, *Algorithms and Autonomy: The Ethics of Automated Decision Systems* (Cambridge: Cambridge University Press, 2021), <https://doi.org/10.1017/9781108895057>.

⁸¹ Rubel, Castro, and Pham.

⁸² Rubel, Castro, and Pham.

⁸³ Rubel, Castro, and Pham.

⁸⁴ Jonny Thomson, "Algocracy Would Replace Politicians with Algorithms. Should We Try It?," Big Think, November 28, 2022, <https://bigthink.com/thinking/algocracy-algorithm-government/>.

⁸⁵ Dattani, "Big Brother Is Scanning."

⁸⁶ Benson, "The Danger of License Plate Readers in Post-Roe America."

ALPRs are susceptible to bias from factors like a car's make and model or the vehicle's geographic location. Vehicle license plates captured in high-crime areas may draw greater suspicion than vehicles in low-crime areas.⁸⁷ For example, individuals who attended a Black Lives Matter protest in Long Beach were stopped by police and held at gunpoint and had their vehicle seized after police flagged their vehicle in an ALPR database.⁸⁸ ALPR cameras have also misread license plates, anomalies that further support the necessity of confirming the data.⁸⁹ Overall, algocracy theory serves as a prescriptive model for analyzing the disparate impact of ALPR expansion programs and the use of such technologies in law enforcement surveillance operations. It can also be used to identify ways to mitigate some of the adverse effects of algorithmic decision-making.

E. MOSAIC THEORY AS AN APPLIED FRAMEWORK

Expanding police ALPR programs challenges cherished privacy rights in the United States. Ubiquitous police surveillance also raises privacy concerns as civil liberties can be “chilled” by government overreach.⁹⁰ According to Sarah Brayne, “The lines between public and private have become blurry as the state becomes more reliant on private surveillance platforms to facilitate surveillance work.”⁹¹ Law enforcement needs to strike a balance between the need to gather information for criminal investigations and the need to protect individual rights and freedoms.⁹² Privacy rights are uniquely safeguarded as police departments rely on third-party technological offerings, such as predictive policing algorithms, and use data integration platforms in their daily operations.⁹³ Therefore, the

⁸⁷ McConlogue, “Discrimination on Wheels.”

⁸⁸ McConlogue.

⁸⁹ Wesner and Blevins, “Restraining the Surveillance Society.”

⁹⁰ Joh, “Policing the Smart City”; Lauren Fash, “Automated License Plate Readers: The Difficult Balance of Solving Crime and Protecting Individual Privacy,” *Maryland Law Review Endnotes* 78 (2019): 63–98, <https://digitalcommons.law.umaryland.edu/endnotes/59/>.

⁹¹ Sarah Brayne, “The Banality of Surveillance,” *Surveillance & Society* 20, no. 4 (2022): 372–78, <https://doi.org/10.24908/ss.v20i4.15946>.

⁹² Michael Nutt, Qing Yang, and Song Fu, “PlateGuard: License Plate Privacy Protection for Internet of Vehicles,” in *Proceedings of the Fourth International Conference on Connected and Autonomous Driving (MetroCAD)* (Piscataway, NJ: IEEE, 2021), 41–47, <https://doi.org/10.1109/MetroCAD51599.2021.00015>.

⁹³ Brayne, “The Banality of Surveillance.”

need to balance privacy demands with emerging technologies is especially relevant to this discussion, which is outlined in the following subsections.

1. ALPR Privacy

The use of ALPRs has raised concerns about privacy and civil liberties, as these systems can track vehicle movements without owners' knowledge or consent.⁹⁴ Brayne considers ALPR systems "dragnet surveillance tools—they take everyone [that passes the camera], not just people under suspicion."⁹⁵ This indiscriminate collection has led to legal challenges and debates over law enforcement's appropriate use of ALPRs.⁹⁶

As a result, law enforcement surveillance programs must meet rigorous legal and regulatory requirements, such as search warrants and court orders, designed to ensure the lawful and appropriate use of surveillance. Additionally, legal debates have considered the appropriate level of surveillance and the trade-offs between security and privacy in democratic societies.⁹⁷ In order to maintain public trust, law enforcement surveillance programs must be responsibly deployed and follow all the required legal mandates.

2. ALPRs and Civil Liberties

The use of ALPRs raises concerns about privacy and civil liberties because there has been law enforcement overreach within these programs. For example, law enforcement agencies collect and store vast amounts of data on vehicle movements without any apparent justification or legal authority.⁹⁸ These data can be used to track the movements of individuals under no criminal suspicion and are often retained for long periods.⁹⁹ Stored data continue to be a point of contention, as there is no legal standard in the United States, and retention periods vary by state.

⁹⁴ Brooks, "Drawing the Lines."

⁹⁵ Brayne, "Big Data Surveillance," 979.

⁹⁶ Brooks, "Drawing the Lines."

⁹⁷ Nutt, Yang, and Fu, "PlateGuard."

⁹⁸ "California Automated License Plate Reader Policies," Electronic Frontier Foundation, accessed September 6, 2023, <https://www EFF.org/pages/california-automated-license-plate-reader-policies>.

⁹⁹ Friedman et al., "Policing Police Tech."

3. ALPR Data Sharing

ALPR data are often shared between law enforcement agencies and other government entities, including immigration enforcement agencies.¹⁰⁰ While cross-reporting and information sharing optimize law enforcement surveillance programs, this practice has led to targeting individuals based on geolocation or other personal information.¹⁰¹ According to Slobogin and Brayne, “The most common use of ALPRs is to store license plate data for potential use during future investigations.”¹⁰² Typically, police officers learn about crimes after they are committed, prompting them to review ALPR data for evidence collection and confirm suspects’ statements. The information generated by ALPRs provides law enforcement with a citywide vehicle distribution map and, in certain instances, allows authorities to deduce drivers’ habitually traveled routes or speculate on their geolocation by analyzing vehicles’ overnight parking spots.¹⁰³ When the technology is used responsibly, police can leverage ALPR data sharing as a powerful resource.

4. Misuse of ALPR Data

Law enforcement officials sometimes misappropriate ALPR data for personal or political purposes.¹⁰⁴ A police lieutenant from the Metropolitan Police Department of the District of Columbia pleaded guilty to extortion after he admitted to using ALPRs to uncover the owners of vehicles parked outside a gay nightclub and extort them.¹⁰⁵ A former Everett, Washington, police officer was arrested after he accessed an ALPR database to track a woman and frame her boyfriend with false narcotics charges to end their relationship.¹⁰⁶ Long Beach police officers used ALPR cameras to track the movements of

¹⁰⁰ McConlogue, “Discrimination on Wheels.”

¹⁰¹ McConlogue.

¹⁰² Christopher Slobogin and Sarah Brayne, “Surveillance Technologies and Constitutional Law,” *Annual Review of Criminology* 6, no. 1 (2023): 221, <https://doi.org/10.1146/annurev-criminol-030421-035102>.

¹⁰³ Slobogin and Brayne.

¹⁰⁴ Electronic Frontier Foundation, “Street-Level Surveillance.”

¹⁰⁵ Fash, “The Difficult Balance of Solving Crime and Protecting Individual Privacy.”

¹⁰⁶ Hofer, “The Pitfalls of Law Enforcement License Plate Readers.”

motorists attending Black Lives Matter protests after their vehicles were parked near a looting scene.¹⁰⁷ Such abuse of power is particularly concerning for motorists who live in high-crime areas, where street parking exposes them to greater police surveillance. The over-indexing from ALPRs in high-crime areas can draw heightened suspicion of motorists who live in those neighborhoods. Prolonged surveillance came under scrutiny in the *United States v. Jones* case.¹⁰⁸ The Supreme Court held that installing a 30-day GPS tracker on the defendant's car, which was then used to track his vehicle movements to locate his narcotic supplies, constituted an unreasonable search and violated his Fourth Amendment rights.¹⁰⁹ The *Jones* case prompted the courts to provide legal protections under the mosaic theory to safeguard against certain types of long-term, continuous surveillance using technologies such as ALPRs.

Mosaic theory advances the idea that even publicly obtained information about individuals can merit privacy claims.¹¹⁰ The courts have applied the mosaic theory as a legal framework to discourage mass ALPR surveillance programs and provide further protection for private citizens. Mosaic theory proposes that disparate and seemingly innocuous vehicle data obtained by ALPRs can have far-reaching privacy implications when analyzed in the aggregate.¹¹¹ Aggregated sums are more substantial than individual parts, and the amalgamation of those parts should be protected under the Fourth Amendment. Historically, private citizens have lacked a reasonable expectation of privacy in public places. However, practical limitations for tracking the location of private citizens have been well established; neither an average person nor a well-resourced police department can be omnipresent and monitor a person's every move.¹¹² Collecting and analyzing geolocation data from ALPRs yield detailed insights into individuals' private

¹⁰⁷ McConlogue, "Discrimination on Wheels."

¹⁰⁸ Schlabach, "Privacy in the Cloud."

¹⁰⁹ "Criminal Procedure—Fourth Amendment—Massachusetts Supreme Judicial Court Holds That Use of Automated License Plate Readers May Constitute a Search—*Commonwealth v. McCarthy*, 142 N.E.3d 1090 (Mass. 2020)," *Harvard Law Review* 134, no. 8 (June 2021): 2887–94, EBSCO.

¹¹⁰ Bryce Clayton Newell, Tjerk Timan, and Bert-Jaap Koops, eds., *Surveillance, Privacy and Public Space* (London: Routledge, 2018), <https://doi.org/10.4324/9781315200811>.

¹¹¹ Schlabach, "Privacy in the Cloud."

¹¹² Newell, Timan, and Koops, *Surveillance, Privacy and Public Space*.

lives.¹¹³ Combined with vehicle record checks, these fragmented pieces of geolocation data can reveal personal preferences and record driving patterns that otherwise would have been private.¹¹⁴ Unfortunately, warrantless access to stored vehicle data, a once powerful investigative tool, is no longer available to law enforcement under the protections of the mosaic theory.

F. CONCLUSION

Emerging technologies like ALPR cameras blur the lines between public and private spaces.¹¹⁵ ALPR police cameras accumulate massive amounts of geolocation data, stored in large databases until they become relevant in active criminal investigations. Meanwhile, the corporate surveillance economy has expanded without any regulatory controls. Vehicle data are collected, sold, and brokered with little consumer oversight.¹¹⁶ Law enforcement's relationship with the Fourth Amendment and technology is fraught with legal complexity, which demands privacy rights be balanced against the need to expand police surveillance programs for public safety. The Supreme Court introduced the mosaic theory as one way to curtail prolonged electronic surveillance of suspects' movements over time.¹¹⁷ This theory serves as a viable framework to create the necessary safety guardrails as more police departments expand ALPR programs. As technology advances and more police agencies develop ALPR programs, the courts and legal scholars will put data retention and privacy laws to the test.¹¹⁸ Chapter III examines data retention and privacy challenges more closely.

¹¹³ Schlabach, "Privacy in the Cloud."

¹¹⁴ Bedi, "Social Networks, Government Surveillance."

¹¹⁵ Brayne, "The Banality of Surveillance."

¹¹⁶ McConlogue, "Discrimination on Wheels."

¹¹⁷ Bedi, "Social Networks, Government Surveillance."

¹¹⁸ Bedi.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DATA PRIVACY

The pervasiveness and normalization of ALPR surveillance cameras throughout urban landscapes have piqued the interest of privacy advocates and law enforcement professionals who are entrusted with maintaining data privacy. This chapter explores the complex and increasingly critical domain of data privacy in ALPR expansion programs. To understand the significance of personal data as the new “gold” of the 21st century digital economy, this chapter reviews best practices that govern data retention standards and highlights privacy issues when collecting ALPR data. From stringent regulatory frameworks to sophisticated encryption technologies, this chapter explores the multilayered data privacy landscape, the ethical implications it presents, and its profound impact on an increasingly interconnected society. It also presents comparative case study analysis to contrast variable data retention policies in the United States and the United Kingdom. These case studies not only illustrate the impact of variable data retention policies on data privacy but also provide guidance for future regulatory frameworks. Understanding data privacy is a technical necessity as well as a fundamental aspect of ensuring that individual rights and freedoms are protected when expanding ALPR programs.

A. VARIABLE DATA RETENTION STANDARDS

Codifying data retention standards in the United States is a multidimensional, complex problem involving numerous state and local governments. Police departments in the United States have vastly different data retention policies and regulations, which can lead to inconsistencies in the protection of individual privacy and data security.¹¹⁹ Even under the best circumstances, police departments are vulnerable to hacks and data breaches.¹²⁰ In 2019, an unauthorized ALPR data leak by a U.S. Customs and Border

¹¹⁹ Lum et al., “The Rapid Diffusion of License Plate Readers.”

¹²⁰ “Insecure License Plate Readers Could Be Exposing the Data of Millions of Drivers,” Insure Trust, accessed July 19, 2023, <https://insuretrust.com/2019/03/20/insecure-license-plate-readers-could-be-exposing-the-data-of-millions-of-drivers/>.

contractor exposed 50,000 license plates and reenergized the debate on ALPR data security and better privacy controls.¹²¹

Law enforcement agencies aggregate massive amounts of ALPR data in large, regional databases.¹²² However, there are no federal guidelines for data retention standards in the United States, so policies vary by state.¹²³ Additionally, police purchase and retain ALPR data from third-party vendors like Vigilant Solutions, which has collected five billion license plates from around the country.¹²⁴ Such arrangements become more interesting as law enforcement agencies store ALPR data differently for interstate commuters, and their data retention policies vary depending on the jurisdiction. In the absence of uniform federal guidelines, police departments defer to their own data retention policies.¹²⁵ Law enforcement experts are still uncertain about the best data storage practices.¹²⁶ For example, New Hampshire purges ALPR data after three minutes while Georgia stores data for 30 months.¹²⁷ Meanwhile, California retains such data no longer than 60 days unless they are actively used in criminal investigations (see Table 1 for California’s related data retention and privacy laws).¹²⁸ However, according to the EFF, the storage of ALPR data unrelated to a particular crime has been contested by privacy advocates in California.¹²⁹ Indeed, ALPR system databases record every license plate read,

¹²¹ Kevin Collier and Sergio Hernandez, “At Least 50,000 License Plates Leaked in Hack of Border Contractor Not Authorized to Retain Them,” CNN, June 17, 2019, <https://www.cnn.com/2019/06/17/politics/customs-and-border-protection-data-breach-license-plates-leaked/index.html>.

¹²² Friedman et al., “Policing Police Tech.”

¹²³ Wesner and Blevins, “Restraining the Surveillance Society.”

¹²⁴ Angel Diaz and Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use* (New York: Brennan Center for Justice, 2020), <https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations>.

¹²⁵ Friedman et al., “Policing Police Tech.”

¹²⁶ Lum et al., “The Rapid Diffusion of License Plate Readers.”

¹²⁷ “Automated License Plate Readers: State Statutes,” National Conference of State Legislatures, February 3, 2022, <https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx>.

¹²⁸ Cal. Veh. Code § 2413 (2011) https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=VEH§ionNum=2413.

¹²⁹ Maass and Tsukayama, “EFF Joins Effort to Restrict ALPRs.”

even those not on a hotlist, in a searchable format for future record query.¹³⁰ As a result, many privacy advocates argue that law enforcement could easily track individuals by accessing and analyzing their geolocation data, which could lead to Fourth Amendment violations.¹³¹

Table 1. California’s ALPR Data Retention and Privacy Laws.¹³²

California (2011) Calif. Veh. Code § 2413	Provides that the California Highway Patrol (CHP) may retain data from a license plate reader for no more than 60 days unless the data is being used as evidence in felony cases. Prohibits selling or making ALPR data available to non-law enforcement officers or agencies. Requires CHP to report to the legislature how ALPR data is being used.
California (2015) Calif. Civil Code §§ 1798.29, 1798.90.5	Establishes regulations on the privacy and usage of automatic license plate recognition (ALPR) data and expands the meaning of “personal information” to include information or data collected through the use or operation of an ALPR system. Imposes privacy protection requirements on entities that use ALPR information, as defined; prohibits public agencies from selling or sharing ALPR information, except to another public agency, as specified; and requires operators of ALPR systems to use that information only for authorized purposes.

The 2021–2022 California State Senate proposed new legislation under S.B. 210 that would further tighten the state’s 2015 privacy laws. The law would require California law enforcement officers to purge and delete ALPR data after 24 hours unless the vehicle is associated with a hot list.¹³³ It would also prevent law enforcement from accessing ALPR data beyond 24 hours. Additionally, it would require annual audits to ensure ALPR data

¹³⁰ Diaz and Levinson-Waldman, *Legal Status and Policy Recommendations for Law Enforcement*.

¹³¹ Keith Gierlack et al., *License Plate Readers for Law Enforcement: Opportunities and Obstacles* (Santa Monica, CA: RAND Corporation, 2014), https://www.rand.org/pubs/research_reports/RR467.html.

¹³² Source: National Conference of State Legislatures, “State Statutes.”

¹³³ “2022—Senate Bill 210 (Wiener, Scott), Automated License Plate Recognition Systems: Use of Data (Dead),” California Air Resources Board, accessed August 3, 2023, <https://ww2.arb.ca.gov/2022-senate-bill-210-wiener-scott-automated-license-plate-recognition-systems-use-data-dead>.

are deleted.¹³⁴ Although S.B. 210 was one of the most aggressive attempts to enforce stricter ALPR guidelines, the bill failed in the California State Senate.¹³⁵

To address the variability of data retention standards, DHS solicited bids in February 2014 to create a national database of data gathered through ALPR systems.¹³⁶ While DHS's proposal was eventually canceled, the bid solicitation demonstrated how pervasive the database would have been if realized. Discrepancies in data retention laws allow the ALPR industry to go unregulated. Using ALPR technology in data collection and analysis has spurred the debate for better data hygiene and stronger constitutional protections.

In stark contrast to the United States, the United Kingdom enjoys more broad acceptance of ALPR technology. In the early 1990s, the UK installed automatic number plate recognition (ANPR) surveillance cameras “after a bombing campaign by Northern Irish terrorists left four people dead, dozens injured, and parts of the City of London in ruins.”¹³⁷ ANPR technology has been deployed in the UK since the late 1970s, primarily by law enforcement agencies, to aid in detecting and preventing crime. Unlike the controversy surrounding ALPR use in the United States, the British public generally accepts the technology as a necessary tool for maintaining public safety and security.¹³⁸

One reason for widespread public acceptance in the UK involves cultural attitudes toward privacy. The United States has a strong cultural emphasis on individual rights and freedoms, which are highlighted in the U.S. Constitution under the Fourth Amendment. Concerns about privacy and potential governmental overreach greatly influence American attitudes toward surveillance. Additionally, the regulatory environment in the UK provides

¹³⁴ Maass and Tsukayama, “EFF Joins Effort to Restrict ALPRs.”

¹³⁵ Zach Boetto, “Millions of License Plates Are Scanned in Order to Combat Crime. Is Storing That Information a Violation of Privacy?,” FOX 40 Sacramento, September 14, 2022, <https://fox40.com/news/fox40-focus/license-plate-readers-alpr-privacy-police-california/>.

¹³⁶ Dryer and Stroud, “Automatic License Plate Readers.”

¹³⁷ Justin Mullins, “Ring of Steel II—New York City Gets Set to Replicate London’s High-Security Zone,” *IEEE Spectrum* 43, no. 7 (July 2006): 12–13, <https://doi.org/10.1109/MSPEC.2006.1652996>.

¹³⁸ “How London Became the World’s CCTV Capital,” *The Age*, July 26, 2005, <https://www.theage.com.au/national/how-london-became-the-world-s-cctv-capital-20050726-ge0ksv.html>.

some assurance to the public that there are checks and balances on how data are used. ANPRs in the UK are not just for security; they are also used for tasks like speed enforcement and traffic management.¹³⁹ The public sees this multifaceted use of ALPR technology as beneficial rather than duplicitous.

The primary legislation governing ANPR use in the UK is the 2018 Data Protection Act, which established clear guidelines for collecting, storing, and using personal data, including license plate numbers.¹⁴⁰ The act requires organizations using ANPR technology have a lawful basis for processing the data and ensures that such data are used fairly, transparently, and for a specific purpose. As explained by Roberts and Casanova, “The UK classified ANPR data as *personal data* and follows eight data protection principles articulated in their Data Protection Act.”¹⁴¹ The subsequent list enumerates a few of the guiding principles:

1. Lawfulness, fairness, and transparency: Personal data must be processed lawfully, fairly, and in a transparent manner.
2. Purpose limitation: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in an incompatible manner.
3. Data minimization: Personal data must be adequate, relevant, and limited to what is necessary in the purposes for which they are processed.
4. Accuracy: Personal data must be accurate and, where necessary, kept up to date. Inaccurate data should be corrected or erased without delay.
5. Storage limitation: Personal data must not be kept for longer than is necessary for the purposes for which they are processed.

¹³⁹ “ANPR for UK,” *Plate Recognizer* (blog), May 3, 2022, <https://platerecognizer.com/anpr-for-uk/>.

¹⁴⁰ Wesner and Blevins, “Restraining the Surveillance Society.”

¹⁴¹ David J. Roberts and Meghann Casanova, *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement* (Alexandria, VA: International Association of Chiefs of Police, 2012), <https://trid.trb.org/view/1223372>.

6. Integrity and confidentiality: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.¹⁴²

In addition to the 2018 Data Protection Act, the UK successfully scaled up ANPR programs by establishing a national ANPR database to cross-reference, identify and apprehend criminals, particularly those involved in serious or organized crime. Approximately 13,000 ANPR cameras detect vehicle movements in the UK, submitting around 55 million records per day to the national ANPR database.¹⁴³ Within London’s sprawling financial district, the thousands of interconnected closed-circuit cameras that observe pedestrian and vehicle traffic are known as the ring of steel.¹⁴⁴ The technology can quickly and accurately read license plates and cross-reference them within the national databases of known vehicles and their owners. As police departments expand ALPR surveillance programs in the United States, it is helpful to examine existing data retention policy models in the UK to establish best practices.

B. COMPARATIVE ALPR POLICY CASE STUDIES

ALPR technology has become an integral surveillance tool for law enforcement agencies across the United States. However, the adoption and use of ALPR technology have not been standardized across the nation. Different jurisdictions have established variable policies governing data retention, storage, and use of ALPR systems. This variability underscores the broader debate about balancing public safety with individual privacy rights and prompts a closer examination of the diverse ALPR policies in place across the United States. The following analysis examines the legal underpinnings of four U.S. police departments’ ALPR programs representing the various cross-sections of local and state police agencies in California—the Glendale Police Department, the Beverly Hills

¹⁴² Data Protection Act of 2018, c. 12 (UK), <https://www.legislation.gov.uk/ukpga/2018/12/part/4/chapter/2/enacted>; “Data Protection,” UK Government Digital Service, accessed April 16, 2023, <https://www.gov.uk/data-protection>.

¹⁴³ “ANPR for UK.”

¹⁴⁴ Mullins, “Ring of Steel II.”

Police Department, and the California Highway Patrol—and one outside agency—the Metropolitan Police Department of the District of Columbia—juxtaposed with policies in the UK (see Table 2 for a concise comparison).

The Metropolitan Police Department of the District of Columbia defines its license plate reader (LPR) data retention and administration in General Order 303.09:

1. Portable LPR data will be stored *up to 30 days* on the MDC [Metropolitan Police Department of the District of Columbia] after which time the LPR system will overwrite the data on the MDC [emphasis added]. LPR data shall be stored *for a period of 90 days* and then destroyed unless the LPR data results in a verified, positive hit [emphasis added]. Such data shall be retained for a period of one year and then destroyed.
2. Members seeking LPR images or data for investigative purposes shall submit at a request to the Investigative Support Section (ISS) at mpdcrs@dc.gov. ISS shall provide a response to the requesting member within 24 hours. Members shall ensure all images and data are appropriately uploaded in the investigative file and evidence.com.
3. The LPR program manager shall ensure that all LPR data covered by a litigation hold, relevant to pending litigation, or reasonably suspected to be relevant to future litigation are retained in evidence.com until notified that the subject litigation has concluded.¹⁴⁵

The Glendale Police Department's ALPR collection and retention policy appears in its *Policy Manual* under Section 431.5:

The Administrative Services Division Commander is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

All ALPR data downloaded to the server should be stored for a *minimum of one year* (Government Code § 34090.6) and in accordance with the established records retention schedule [emphasis added]. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those

¹⁴⁵ Metropolitan Police Department of the District of Columbia, *License Plate Reader Program*, GO-OPS-303.09 (Washington, DC: Metropolitan Police Department of the District of Columbia, 2014), 6, https://go.mpdconline.com/GO/GO_303_09.pdf.

circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.¹⁴⁶

The Beverly Hills Police Department's ALPR collection and retention policy appears in its *Policy Manual* under Section 429.5:

The Administrative Services Division Commander is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

All ALPR data downloaded to the server should be stored for a *minimum of thirteen months (395 days)* (Government Code § 34090.6) and in accordance with the established records retention schedule [emphasis added]. In cases where it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records, the applicable data should be downloaded from the server onto portable media and booked into evidence.¹⁴⁷

The California Highway Patrol's LPR administrative, retention, and disclosure policy appears in Cal. Veh. Code § 2413:

(a) The Commissioner of the California Highway Patrol is designated as the Statewide Vehicle Theft Investigation and Apprehension Coordinator. The commissioner may establish vehicle theft prevention, investigation, and apprehension programs. The commissioner may assist local, state, and federal law enforcement agencies by coordinating multijurisdictional vehicle theft investigations and may establish programs to improve the ability of law enforcement to combat vehicle theft.

(b) The Department of the California Highway Patrol may retain license plate data captured by a license plate reader (LPR) *for no more than 60 days*, except in circumstances when the data is being used as evidence or for all felonies being investigated, including, but not limited to, auto theft, homicides, kidnapping, burglaries, elder and juvenile abductions, Amber Alerts, and Blue Alerts [emphasis added].

¹⁴⁶ Glendale Police Department, *Policy Manual* (Glendale, CA: Glendale Police Department, 2023), 448, <https://www.glendaleca.gov/home/showpublisheddocument/54469/638169116046230000>.

¹⁴⁷ Beverly Hills Police Department, *Policy Manual* (Beverly Hills: Beverly Hills Police Department, 2018), 277, [http://www.beverlyhills.org/cbhfiles/storage/files/344412877926870728/BeverlyHillsPoliceDepartmentPolicyManual\(11-2018\).pdf](http://www.beverlyhills.org/cbhfiles/storage/files/344412877926870728/BeverlyHillsPoliceDepartmentPolicyManual(11-2018).pdf).

(c) The Department of the California Highway Patrol 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.

(d) The Department of the California Highway Patrol shall monitor internal use of the LPR data to prevent unauthorized use.

(e) The Department of the California Highway Patrol shall, as a part of the annual automobile theft report submitted to the Legislature pursuant to subdivision (b) of Section 10901, report the LPR practices and usage, including the number of LPR data disclosures, a record of the agencies to which data was disclosed and for what purpose, and any changes in policy that affect privacy concerns.¹⁴⁸

The Home Office delineates the UK's national record deletion policy for ANPRs in its *National ANPR Standards*:

ANPR READ [the interpretation of a vehicle registration mark] records must be deleted *12 months after their initial capture*, unless retained under provisions of the criminal procedure investigations act (CPIA) or similar provisions in Scotland [emphasis added]. Retained data may only be accessed in connection with the investigation subject to that retention after a period of 12 months following initial capture.¹⁴⁹

Moreover, as described by the Home Office on its Police.UK website,

Staff only have access to data if it's relevant to their role. Most of those who have permission may only do so for *a maximum of 90 days* from the date it was collected [emphasis added].

For serious, major or counter terrorism investigations some staff may be given access to data for up to one year, subject to authorization of a senior officer.¹⁵⁰

¹⁴⁸ Cal. Veh. Code § 2413.

¹⁴⁹ Home Office, *National ANPR Standards for Policing and Law Enforcement* (London, Home Office, 2022), 34, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091167/NASPLE_Version_2.4_July_2022.pdf.

¹⁵⁰ "Automatic Number Plate Recognition (ANPR)," Home Office, accessed July 18, 2023, <https://www.police.uk/advice/advice-and-information/rs/road-safety/automatic-number-plate-recognition-anpr/>.

Furthermore, the Home Office describes the UK's ANPR retention policy in its *National ANPR Standards*:

Records may also be retained for *longer than 12 months* following a review that identifies a continuing policing purpose for those items of data under the provisions of the management of police information [emphasis added]. These records must be retained and managed in accordance with those provisions. Law enforcement agencies must establish procedures for the management and review of any data held under these provisions including arrangements for deletion as required.¹⁵¹

Table 2. Summary of Police Data Retention Periods and Dispositions

Police Department	Data Retention (personnel access)	Data Disposition
Glendale PD	30 days	1 year
Beverly Hills PD	395 days	13 months
California Highway Patrol	60 days	60 days
Metropolitan Police Department (DC)	30 days	90 days
UK Home Office	90 days	1 year

Uniformity in ALPR data retention policies offers a range of benefits, from streamlined law enforcement operations to enhanced public trust. Consistent data retention policies across jurisdictions allow police agencies to adhere to a standard, eliminating the complexity and confusion caused by variable retention timelines. Such uniformity can facilitate better interagency cooperation, allowing for smoother ALPR data sharing and collaboration in multi-jurisdictional cases. For example, if the United States had a standardized one-year data retention policy, the Glendale Police Department could access ALPR data from DC Metro beyond its current 90-day retention policy. From a public perspective, a standardized data retention policy increases transparency and predictability,

¹⁵¹ Home Office, *National ANPR Standards*, 34.

helping citizens understand their data privacy rights and what to expect regarding ALPR data preservation. Moreover, consistent guidelines can reduce potential legal challenges or disputes related to data misuse or over-retention, ensuring ALPR surveillance technology is used effectively while respecting privacy concerns.

In comparing the four different U.S. police departments to the national standard in the UK, the apparent variability among data retention policies becomes clear. The Beverly Hills Police Department retains data for the longest period, 13 months, while CHP purges data every 60 days. The Beverly Hills Police Department covers a smaller, more affluent jurisdiction with less bureaucracy than CHP, one of the largest police agencies in California. CHP is led by a commissioner who must navigate the complexity of state-level governance. Meanwhile, the Beverly Hills Police Department enjoys broad community support of its ALPR surveillance programs.¹⁵² The Beverly Hills Police Department can access stored ALPR data for 13 months, affording police detectives more time to conduct thorough criminal investigations. The UK's uniform national data retention policy allows 90-day authorized personnel access and disposes ALPR data within one year. Allowing such retention is especially important as criminal investigations often require researching ALPR databases after a crime is committed. Thus, codifying data retention standards can positively impact criminal investigations for future crimes, when researching stored ALPR databases will be essential to solving them.

C. DATA SECURITY

Storing data for longer periods requires enhanced security measures to safeguard citizens' privacy and avoid data leaks. Although there are no established guidelines for ALPR cloud storage, the digital security industry recognizes the 256-bit Advanced Encryption Standard (AES) as the most secure data storage available.¹⁵³ This encryption refers to the process of blocking plain text data using the AES algorithm and key length of

¹⁵² Patrick Sisson, "In (and above) Beverly Hills, Police Are Watching," Bloomberg, January 19, 2023, <https://www.bloomberg.com/news/features/2023-01-19/in-beverly-hills-police-surveillance-technology-takes-off>.

¹⁵³ Joan Daemen and Vincent Rijmen, *The Design of Rijndael: The Advanced Encryption Standard (AES)*, 2nd ed. (Cham, Switzerland: Springer, 2020).

256 bits. This security process is considered the most mathematically complex and most challenging code to decipher. According to Daniel, “AES encryption is a symmetric encryption algorithm because it uses one key for encryption and decryption.”¹⁵⁴ Privacy advocates recommend that ALPR software adhere to such industry standards because information transmitted via AES 256-bit encryption is virtually impenetrable and offers the highest security detection (see Figure 1).

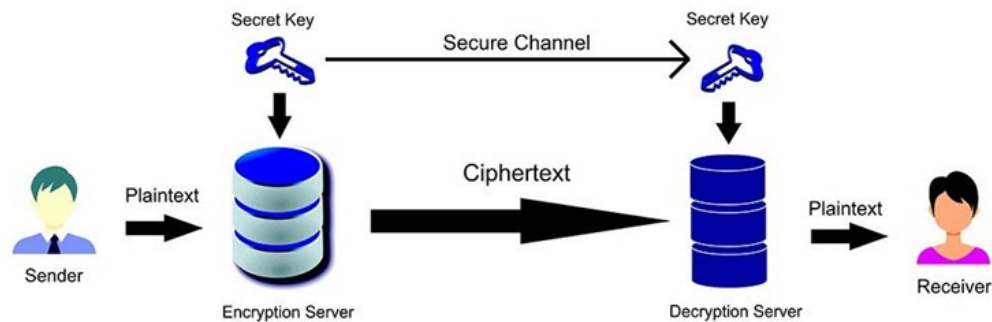


Figure 1. Symmetric Cryptography.¹⁵⁵

Standardized data encryption remains a central debate among security professionals. Police ALPR databases are not impervious to cyberattacks. A well-known 2015 security breach compromised Boston’s city ALPR system, revealing driver and vehicle information dating back to 2012.¹⁵⁶ One recommendation following this breach involved regular data hygiene and purging of non-pertinent data. Data breaches not only erode public trust, but they also have homeland security implications. Without proper security protocols, nefarious actors can illegally access ALPR databases, causing this technology to be used for unlawful purposes. Poorly secured ALPR databases can be hacked by terrorists to conduct surveillance on high-value targets. In a 2019 independent

¹⁵⁴ Brett Daniel, “What Is AES Encryption? [The Definitive Q&A Guide],” Trenton Systems, March 31, 2021, <https://web.archive.org/web/20220801000000/https://www.trentonsystems.com/blog/aes-encryption-your-faqs-answered>.

¹⁵⁵ Source: Daniel.

¹⁵⁶ Insure Trust, “Insecure License Plate Readers.”

study, TechCrunch found that nearly 150 ALPR cameras from various manufacturers were still accessed with default passwords listed in the owner's manuals.¹⁵⁷ It bears mentioning that shared passwords can be accessed by criminals who later extort victims for profit. As previously discussed, good data hygiene helps ensure compliance with data privacy laws. It can prevent unauthorized access, misuse of data, or accidental security breaches resulting in unnecessary fines.¹⁵⁸ Building on the importance of secure ALPR systems, the next section delves deeper into the best practices of scaling up ALPR programs while safeguarding data privacy.

D. FUTURE OUTLOOK FOR ALPR EXPANSION PROGRAMS

Expanding law enforcement ALPR programs has a tangible benefit in collecting and sharing that data for police officers to use in future investigations. Highly integrated computer networks afford police departments greater access to larger ALPR data repositories.¹⁵⁹ These robust network platforms enhance police surveillance operations by scaling ALPR programs beyond local jurisdictions.¹⁶⁰ Private ALPR vendors like Flock Safety already have well-established operating platforms and lease ALPR devices to the government and private businesses. Additionally, law enforcement encourages private citizens to register and share their cameras with police departments to assist with criminal investigations.¹⁶¹ Marketed to homeowners' associations, universities, and law enforcement agencies, these cameras are force multipliers in crime reduction.¹⁶² Police departments consider public safety part of their primary duties, and they purchase such innovative, emerging technologies to ensure community safety.¹⁶³

¹⁵⁷ Zack Whittaker, "Police License Plate Readers Are Still Exposed on the Internet," TechCrunch, January 22, 2019, <https://techcrunch.com/2019/01/22/police-alpr-license-plate-readers-accessible-internet/>.

¹⁵⁸ Gilmartin and Childe, "Developing a Data Retention Policy."

¹⁵⁹ Koper and Lum, "Large-Scale License Plate Reader Deployment."

¹⁶⁰ Koper and Lum.

¹⁶¹ Ashley Johnson, Eric Egan, and Juan Londoño, *Police Tech: Exploring the Opportunities and Fact-Checking the Criticisms* (Washington, DC: Information Technology & Innovation Foundation, 2023), <https://itif.org/publications/2023/01/09/police-tech-exploring-the-opportunities-and-fact-checking-the-criticisms/>.

¹⁶² Kelley and Guariglia, "Things to Know before Your Neighborhood Installs an ALPR."

¹⁶³ Friedman et al., "Policing Police Tech."

Access to stored ALPR data in regional databases is a valuable investigative resource that can be shared with other law enforcement agencies for criminal investigations.¹⁶⁴ Data sharing is especially useful as motorists navigate interstate highways and suspects commit crimes outside local and state jurisdictions. Police departments can reduce their infrastructure build costs and increase operational efficiency by layering their intelligence with ALPR live camera streams that are connected to partnering agencies.¹⁶⁵ Once installed, these cameras are linked and networked within the Flock operating system. Scaling up ALPR surveillance programs requires significant investment capital to purchase camera systems, allocate resources and maintain equipment.¹⁶⁶ However, private vendors like Flock provide a path forward to seamlessly expand police ALPR programs and offer real-time intelligence platforms.¹⁶⁷ Thus, responsibly expanding police ALPR programs while ensuring citizens' privacy rights is a viable model.

The UK's ANPR data privacy guidelines can serve as a working framework for police forces to build and expand ALPR programs responsibly in the United States. As outlined in the UK's 2018 Data Protection Act, data privacy impact assessments (DPIAs) are required before a government entity installs new technology.¹⁶⁸ Specifically, a DPIA is a structured design review process that systematically analyzes, identifies, and mitigates data protection risks of any new proposed project or plan that impacts the public.¹⁶⁹ The DPIA process promotes public trust and accountability by acknowledging the unintended consequences of data leaks and privacy concerns. Prioritizing data privacy early in the implementation process and building ALPR networks with data protections by design are

¹⁶⁴ Boetto, "Millions of License Plates Are Scanned."

¹⁶⁵ "FlockOS," Flock Safety, accessed June 12, 2023, <https://www.flocksafety.com/products/flock-os>.

¹⁶⁶ Murat Ozer, "Automatic License Plate Reader (ALPR) Technology: Is ALPR a Smart Choice in Policing?," *Police Journal* 89, no. 2 (2016): 117–32, <https://doi.org/10.1177/0032258X16641334>.

¹⁶⁷ Flock Safety, "FlockOS."

¹⁶⁸ "CCTV and Video Surveillance," UK Information Commissioner's Office, accessed February 27, 2023, <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv/>.

¹⁶⁹ "What Is a DPIA?," UK Information Commissioner's Office, accessed July 21, 2023, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/>.

a responsible way to garner public trust. Additionally, there are financial benefits associated with DPIAs. Identifying problems early on generally means a simpler, less costly solution. DPIAs can reduce recurring data storage costs by minimizing the amount of information collected.

Integrating guidelines like the UK's DPIA model into ALPR expansion programs in the United States could offer a balanced solution that ensures public safety and privacy protection. By foreseeing and managing data protection risks before the deployment of new technologies, law enforcement agencies can not only uphold their commitment to public safety but also maintain the public's trust and respect individual privacy rights. This dual advantage strengthens their operational capabilities while promoting responsible innovation and setting a standard for future technological integration in law enforcement. The final chapter of this thesis offers policy recommendations and explores how those policies may accelerate ALPR technology adoption among U.S. law enforcement agencies.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EXPANDING ALPR PROGRAMS

Law enforcement professionals are increasingly deploying advanced surveillance technologies like ALPR cameras.¹⁷⁰ The benefits of using ALPRs for evidence collection and criminal investigations are well documented.¹⁷¹ Responsibly scaling ALPR surveillance programs in a democratic society remains a balancing act. Extensively gathering and storing ALPR data require the public's confidence in law enforcement's ability to protect and use the information judiciously.¹⁷²

Optimized by machine learning and advanced algorithms, ALPR surveillance technology has rapidly expanded police ALPR programs. Privacy advocates who oppose law enforcement ALPR expansion programs are still doubtful that the technology serves the interests of private citizens.¹⁷³ The mosaic theory provides a legal framework to limit law enforcement's overreliance on ALPR data for criminal investigations. However, data retention periods remain a central point of contention. More research is needed to evaluate the long-term effects of ALPR technology and its future impact on personal civil liberties.

As more ALPR networks expand commercially, the United States will need balanced legislation that allows law enforcement to benefit from the technology while safeguarding consumer privacy. Private industry has aggressively scaled up for-profit business models to promote widespread ALPR data collection databases. DRN willingly sells that information to third parties to capitalize on the ubiquitous data.¹⁷⁴ In light of the compelling privacy concerns arising from the widespread use of ALPR technology, it becomes imperative to establish comprehensive policies aimed at safeguarding individual privacy.

¹⁷⁰ Dryer and Stroud, "Automatic License Plate Readers."

¹⁷¹ Fash, "The Difficult Balance of Solving Crime and Protecting Individual Privacy."

¹⁷² Merola, Lum, and Murphy, "The Impact of License Plate Recognition Technology."

¹⁷³ Maass, "Automated License Plate Readers Threaten Abortion Access."

¹⁷⁴ Maass.

A comparison of U.S. law enforcement and UK privacy policies reveals differing levels of consumer protection. The UK has embraced comprehensive privacy protections while the United States has deferred to individual states and local municipalities for policy guidance.¹⁷⁵ The outcome in the United States is an inconsistent legislative policy that falls short of providing sufficient data protection for individual privacy. The following section identifies key policy recommendations to ensure that police ALPR programs are expanded responsibly with data privacy in mind.

A. U.S. LAW ENFORCEMENT POLICY RECOMMENDATIONS

The varying ALPR data retention standards across the United States represent an intricate puzzle for law enforcement agencies. As ALPR systems collect, process, and store a large quantity of sensitive data, ensuring these systems operate within the boundaries of state and federal data protection laws is crucial. Divergent standards lead to inconsistencies in data protection measures and leave room for potential misuse and violations of individual privacy. Therefore, while challenging, codifying ALPR data retention standards on a national scale is an essential step toward securing privacy rights in the era of automated surveillance. The following six recommendations serve as a national policy framework to responsibly scale police ALPR programs in the United States.

1. Federally Approved Data Retention Period

Establish a 90-day standardized retention period for ALPR data not immediately linked to active criminal investigations. This retention period strikes a balance between investigative needs and privacy concerns. A single, federally approved policy can eliminate legal ambiguities and conflicts arising from variable state or local policies. This policy can reduce the burden on organizations that operate in multiple jurisdictions. For example, local and state agencies participating in regional task forces can defer to federal ALPR policies rather than navigate the complexity of local and state guidelines.

A nationally approved policy can help increase public trust in how governmental agencies retain and use data and mitigate risks associated with data breaches, misuse, or

¹⁷⁵ Wesner and Blevins, “Restraining the Surveillance Society.”

non-compliance. This 90-day data retention policy is also consistent with the data-privacy policy framework outlined in the UK's national ALPR policy. If ALPR data are linked to active criminal investigations, they may be retained for the duration of that investigation. Current evidence preservation laws allow evidence to be maintained through court case disposition. However, police departments should conduct annual reviews of stored ALPR data to ensure their compliance with the retention period and purge data that no longer meet retention criteria.

2. Data Collection

ALPR systems should be used only for legitimate law enforcement purposes, such as locating stolen vehicles, identifying wanted persons, and supporting ongoing investigations. Storing massive amounts of data can result in expensive storage costs and expose the agency to potential data leaks. Responsibly collecting and storing ALPR data relevant to criminal investigations promotes trust and prioritizes data privacy. ALPR systems must also be regularly calibrated to ensure data accuracy. For example, once recovered, stolen vehicles should be removed immediately from ALPR databases. Inaccurate data can lead to unwarranted law enforcement actions and potential legal challenges.

3. Data Access and Sharing

Access to ALPR data should be restricted to authorized law enforcement personnel involved in active investigations. The interoperability of ALPR data is encouraged to optimize and streamline national security efforts. However, all access to ALPR data should be logged and an audit trail maintained. Doing so will ensure accountability and transparency in the system's use. ALPR data should not be shared with third-party entities unless required by law or necessary for a specific investigation.

4. Data Security

All ALPR data stored should be encrypted to protect against unauthorized access. Passwords should be uniquely generated and not shared with others. Regular security audits should be conducted to ensure ALPR data storage systems are protected from external

threats. This audit procedure should include recurring training for authorized personnel who use ALPR data for investigations.

5. Public Engagement and Transparency

Before implementing or expanding ALPR systems, police departments should engage with community members to explain the benefits and address any concerns. Homeowners' association meetings and community security councils are excellent forums to host public hearings. Referenda on local ballots measures are great tools to gauge community sentiment. Police departments should also conduct DPIAs to identify potential risks for using and storing ALPR data. DPIAs prioritize data privacy early in the process, before new ALPR devices are deployed in the community. This recommendation is consistent with the guidelines of DPIA surveys in the UK.

6. Oversight and Accountability

An independent body should oversee the use of ALPR systems, ensuring they are responsibly used and follow established policies and regulations. Mechanisms should also be in place for community members to address concerns and lodge complaints about ALPR usage. These service complaints should generate prompt and thorough investigations.

B. DISCUSSION FOR FUTURE RESEARCH

Given the detailed information that ALPR systems can capture, defining precise periods for data storage is essential. Prolonged retention periods can be advantageous for solving cold cases and undertaking long-term investigations. However, they also present risks regarding data security, privacy, and potential abuse. Additionally, police agencies can incur unnecessary financial impacts for storing bulk data. Uniform standards need to be established to provide clear legal guidelines for the retention and deletion of such data. Striking the right balance between the utility of data for law enforcement purposes and privacy protection is paramount.

In terms of future research, several areas require further investigation. First, comprehensive studies need to be conducted on the societal impact of ALPR technologies, particularly their effect on personal privacy. Second, research should be directed toward

creating a national interoperable ALPR database that can be universally applied, thereby resolving challenges posed by variable privacy standards. Last, more attention must be directed toward developing advanced, secure data storage solutions that comply with current data retention standards.

Given the accelerating pace of ALPR technology, the United States must prepare for a future in which AI-based, algorithmic surveillance is even more prevalent in law enforcement. Innovative data privacy policies, such as the European Union's General Data Protection Regulation, can be the key to reconciling the benefits of ALPR surveillance with the right to privacy. Additionally, incorporating mechanisms for public input and oversight into the deployment of these systems could help establish trust and ensure ALPR technologies align with societal values.

While ALPR surveillance technologies promise to enhance law enforcement capabilities further, they must be accompanied by thoughtful deliberation on data privacy and retention standards. As U.S. law enforcement navigates the digital age, it needs to ensure technological advancements, such as ALPRs, are introduced in a manner that respects and upholds the democratic principles of privacy, transparency, and accountability. Future research should maximize the potential of ALPR surveillance programs while preserving individuals' fundamental rights.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- The Age*. “How London Became the World’s CCTV Capital.” July 26, 2005.
<https://www.theage.com.au/national/how-london-became-the-world-s-cctv-capital-20050726-ge0ksv.html>.
- Alpert, Geoffrey P., Kyle McLean, and Scott Wolfe. “Consent Decrees: An Approach to Police Accountability and Reform.” *Police Quarterly* 20, no. 3 (2017): 239–49.
<https://doi.org/10.1177/1098611117709591>.
- Bedi, Monu. “Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory.” *Boston University Law Review* 94, no. 6 (December 2014): 1809–80. <https://www.bu.edu/bulawreview/files/2014/12/BEDI.pdf>.
- Benson, Thor. “The Danger of License Plate Readers in Post-Roe America.” *Wired*, July 7, 2022. <https://www.wired.com/story/license-plate-reader-alpr-surveillance-abortion/>.
- Beverly Hills Police Department. *Policy Manual*. Beverly Hills: Beverly Hills Police Department, 2018. [http://www.beverlyhills.org/cbhfiles/storage/files/344412877926870728/BeverlyHillsPoliceDepartmentPolicyManual\(11-2018\).pdf](http://www.beverlyhills.org/cbhfiles/storage/files/344412877926870728/BeverlyHillsPoliceDepartmentPolicyManual(11-2018).pdf).
- Bloch-Wehba, Hannah. “Visible Policing: Technology, Transparency, and Democratic Control.” *California Law Review* 109, no. 3 (June 2021): 917–78. <https://www.californialawreview.org/print/visible-policing-technology-transparency-and-democratic-control/>.
- Boetto, Zach. “Millions of License Plates Are Scanned in Order to Combat Crime. Is Storing That Information a Violation of Privacy?” FOX 40 Sacramento, September 14, 2022. <https://fox40.com/news/fox40-focus/license-plate-readers-alpr-privacy-police-california/>.
- Boldrini, Nicoletta. “Algocracy and Surveillance Capitalism: We Live in a World Governed by Algorithms.” *Medium* (blog), May 30, 2017. <https://nicboldrini.medium.com/algocracy-and-surveillance-capitalism-we-live-in-a-world-governed-by-algorithms-abd1f158186a>.
- Brayne, Sarah. “The Banality of Surveillance.” *Surveillance & Society* 20, no. 4 (2022): 372–78. <https://doi.org/10.24908/ss.v20i4.15946>.
- . “Big Data Surveillance: The Case of Policing.” *American Sociological Review* 82, no. 5 (2017): 977–1008. <https://doi.org/10.1177/0003122417725865>.

- Brooks, Julia M. “Drawing the Lines: Regulation of Automatic License Plate Readers in Virginia.” *Richmond Journal of Law and Technology* 25, no. 3 (2019): 1–32. <https://jolt.richmond.edu/drawing-the-lines-regulation-of-automatic-license-plate-readers-in-virginia/>.
- Calacci, Dan, Jeffrey J. Shen, and Alex Pentland. “The Cop in Your Neighbor’s Doorbell: Amazon Ring and the Spread of Participatory Mass Surveillance.” *Proceedings of the ACM on Human-Computer Interaction* 6, no. CSCW2 (November 2022): 400. <https://doi.org/10.1145/3555125>.
- California Air Resources Board. “2022—Senate Bill 210 (Wiener, Scott), Automated License Plate Recognition Systems: Use of Data (Dead).” Accessed August 3, 2023. <https://ww2.arb.ca.gov/2022-senate-bill-210-wiener-scott-automated-license-plate-recognition-systems-use-data-dead>.
- Collier, Kevin, and Sergio Hernandez. “At Least 50,000 License Plates Leaked in Hack of Border Contractor Not Authorized to Retain Them.” CNN, June 17, 2019. <https://www.cnn.com/2019/06/17/politics/customs-and-border-protection-data-breach-license-plates-leaked/index.html>.
- Daemen, Joan, and Vincent Rijmen. *The Design of Rijndael: The Advanced Encryption Standard (AES)*. 2nd ed. Cham, Switzerland: Springer, 2020.
- Daniel, Brett. “What Is AES Encryption? [The Definitive Q&A Guide].” Trenton Systems, March 31, 2021. <https://web.archive.org/web/20220801000000/https://www.trentonsystems.com/blog/aes-encryption-your-faqs-answered>.
- Dattani, Yash. “Big Brother Is Scanning: The Widespread Implementation of ALPR Technology in America’s Police Forces.” *Vanderbilt Journal of Entertainment and Technology Law* 24, no. 4 (2022): 749–85. <https://scholarship.law.vanderbilt.edu/jetlaw/vol24/iss4/3>.
- Diaz, Angel, and Rachel Levinson-Waldman. *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*. New York: Brennan Center for Justice, 2020. <https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations>.
- Dryer, Randy L., and S. Shane Stroud. “Automatic License Plate Readers: An Effective Law Enforcement Tool or Big Brother’s Latest Instrument of Mass Surveillance? Some Suggestions for Legislative Action.” *Jurimetrics* 55, no. 2 (Winter 2015): 225–74. <https://www.jstor.org/stable/24395572>.
- Electronic Frontier Foundation. “California Automated License Plate Reader Policies.” Accessed September 6, 2023. <https://www.eff.org/pages/california-automated-license-plate-reader-policies>.

- . “Street-Level Surveillance: Automated License Plate Readers (ALPRs).” Accessed September 6, 2023. <https://www.eff.org/pages/automated-license-plate-readers-alpr>.
- Fash, Lauren. “Automated License Plate Readers: The Difficult Balance of Solving Crime and Protecting Individual Privacy.” *Maryland Law Review Endnotes* 78 (2019): 63–98. <https://digitalcommons.law.umaryland.edu/endnotes/59/>.
- Flock Safety. “FlockOS.” Accessed June 12, 2023. <https://www.flocksafety.com/products/flock-os>.
- Friedman, Barry, Farhang Heydari, Max Isaacs, and Katie Kinsey. “Policing Police Tech: A Soft Law Solution.” *Berkeley Technology Law Journal* 37, no. 2 (2022): 701–756. <https://lawcat.berkeley.edu/record/1257876>.
- Gierlack, Keith, Shara Williams, Tom LaTourrette, James M. Anderson, Lauren A. Mayer, and Johanna Zmud. *License Plate Readers for Law Enforcement: Opportunities and Obstacles*. Santa Monica, CA: RAND Corporation, 2014. https://www.rand.org/pubs/research_reports/RR467.html.
- Gilmartin, David, and Kerry Childe. “Developing a Data Retention Policy That Meets Privacy Requirements.” ACC Docket, January 2, 2023. <https://docket.acc.com/developing-data-retention-policy-meets-privacy-requirements>.
- Glendale Police Department. *Policy Manual*. Glendale, CA: Glendale Police Department, 2023. <https://www.glendaleca.gov/home/showpublisheddocument/54469/638169116046230000>.
- Harvard Law Review*. “Criminal Procedure—Fourth Amendment—Massachusetts Supreme Judicial Court Holds That Use of Automated License Plate Readers May Constitute a Search—*Commonwealth v. McCarthy*, 142 N.E.3d 1090 (Mass. 2020).” 134, no. 8 (June 2021): 2887–94. EBSCO.
- Hofer, Jonathan. “The Pitfalls of Law Enforcement License Plate Readers in California and Safeguards to Protect the Public.” Independent Institute, August 16, 2022. <https://www.independent.org/publications/article.asp?id=14254>.
- Home Office. “Automatic Number Plate Recognition (ANPR).” Accessed July 18, 2023. <https://www.police.uk/advice/advice-and-information/rs/road-safety/automatic-number-plate-recognition-anpr/>.
- . *National ANPR Standards for Policing and Law Enforcement*. London, Home Office, 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091167/NASPLE_Version_2.4_July_2022.pdf.

- Horrigan, David. "Data Privacy vs. Crime Prevention: The Automated License Plate Recognition Debate." American Bar Association, August 23, 2021. https://www.americanbar.org/groups/tort_trial_insurance_practice/committees/automobile-litigation/data-privacy-vs-crime-prevention/.
- Insure Trust. "Insecure License Plate Readers Could Be Exposing the Data of Millions of Drivers." Accessed July 19, 2023. <https://insuretrust.com/2019/03/20/insecure-license-plate-readers-could-be-exposing-the-data-of-millions-of-drivers/>.
- Joh, Elizabeth E. "Policing the Smart City." *International Journal of Law in Context* 15 (2019): 177–82. <https://doi.org/10.1017/S1744552319000107>.
- Johnson, Ashley, Eric Egan, and Juan Londoño. *Police Tech: Exploring the Opportunities and Fact-Checking the Criticisms*. Washington, DC: Information Technology & Innovation Foundation, 2023. <https://itif.org/publications/2023/01/09/police-tech-exploring-the-opportunities-and-fact-checking-the-criticisms/>.
- Kaye, Kate. "Private Dollars Are Seeding Surveillance Tech across the US." Smart Cities Dive, February 5, 2021. <https://www.smartcitiesdive.com/news/private-dollars-are-seeding-surveillance-tech-across-the-us/594615/>.
- . "Setting Guardrails." Produced by Smart Cities Dive. In *City Surveillance Watch*, February 8, 2021. Podcast, MP3 audio, 58:20. <https://www.smartcitiesdive.com/news/city-surveillance-watch-setting-guardrails/594495/>.
- Kelley, Jason, and Matthew Guariglia. "Things to Know before Your Neighborhood Installs an Automated License Plate Reader." Electronic Frontier Foundation, September 14, 2020. <https://www.eff.org/deeplinks/2020/09/flock-license-plate-reader-homeowners-association-safe-problems>.
- Kirby, Jared. "Federal Judge Rules in Favor of Digital Recognition Network (DRN) in Antitrust Case." DRN, November 9, 2018. <https://drndata.com/news/federal-judge-rules-favor-digital-recognition-network-drn-antitrust-case/>.
- Koper, Christopher S., and Cynthia Lum. "The Impacts of Large-Scale License Plate Reader Deployment on Criminal Investigations." *Police Quarterly* 22, no. 3 (2019): 305–29. <https://doi.org/10.1177/1098611119828039>.
- Littell, Joe, Maggie Smith, and Nick Starck. "The Devil Is in the Data: Publicly Available Information and the Risks to Force Protection and Readiness." Modern War Institute, September 20, 2022. <https://mwi.westpoint.edu/the-devil-is-in-the-data-publicly-available-information-and-the-risks-to-force-protection-and-readiness/>.
- Lum, Cynthia, Christopher S. Koper, James Willis, Stephen Happeny, Heather Vovak, and Jordan Nichols. "The Rapid Diffusion of License Plate Readers in US Law Enforcement Agencies." *Policing* 42, no. 3 (2019): 376–93. <https://doi.org/10.1108/PIJPSM-04-2018-0054>.

- Maass, Dave. “Automated License Plate Readers Threaten Abortion Access. Here’s How Policymakers Can Mitigate the Risk.” Electronic Frontier Foundation, September 28, 2022. <https://www.eff.org/deeplinks/2022/09/automated-license-plate-readers-threaten-abortion-access-heres-how-policymakers>.
- Maass, Dave, and Hayley Tsukayama. “EFF Joins Effort to Restrict Automated License Plate Readers in California.” Electronic Frontier Foundation, March 19, 2021. <https://www.eff.org/deeplinks/2021/01/eff-joins-effort-restrict-automated-license-plate-readers-california>.
- Matskis, Louise. “Can License Plate Readers Really Reduce Crime?” *Wired*, October 24, 2019. <https://www.wired.com/story/flock-safety-license-plate-readers-crime/>.
- McConlogue, Nicole K. “Discrimination on Wheels: How Big Data Uses License Plate Surveillance to Put the Brakes on Disadvantaged Drivers.” *Stanford Journal of Civil Rights & Civil Liberties* 18 (2022): 269–332. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839726.
- Merola, Linda M., Cynthia Lum, and Ryan P. Murphy. “The Impact of License Plate Recognition Technology (LPR) on Trust in Law Enforcement: A Survey-Experiment.” *Journal of Experimental Criminology* 15, no. 1 (March 2019): 55–66. <https://doi.org/10.1007/s11292-018-9332-8>.
- Metropolitan Police Department of the District of Columbia. *License Plate Reader Program*. GO-OPS-303.09. Washington, DC: Metropolitan Police Department of the District of Columbia, 2014. https://go.mpdonline.com/GO/GO_303_09.pdf.
- Mullins, Justin. “Ring of Steel II—New York City Gets Set to Replicate London’s High-Security Zone.” *IEEE Spectrum* 43, no. 7 (July 2006): 12–13. <https://doi.org/10.1109/MSPEC.2006.1652996>.
- Munn, Luke. “Staying at the Edge of Privacy: Edge Computing and Impersonal Extraction.” *Media and Communication* 8, no. 2 (2020): 270–79. <https://doi.org/10.17645/mac.v8i2.2761>.
- National Conference of State Legislatures. “Automated License Plate Readers: State Statutes.” February 3, 2022. <https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx>.
- Newell, Bryce Clayton, Tjerk Timan, and Bert-Jaap Koops, eds. *Surveillance, Privacy and Public Space*. London: Routledge, 2018. <https://doi.org/10.4324/9781315200811>.

- Nutt, Michael, Qing Yang, and Song Fu. "PlateGuard: License Plate Privacy Protection for Internet of Vehicles." In *Proceedings of the Fourth International Conference on Connected and Autonomous Driving (MetroCAD)*, 41–47. Piscataway, NJ: IEEE, 2021. <https://doi.org/10.1109/MetroCAD51599.2021.00015>.
- Ozer, Murat. "Automatic License Plate Reader (ALPR) Technology: Is ALPR a Smart Choice in Policing?" *Police Journal* 89, no. 2 (2016): 117–32. <https://doi.org/10.1177/0032258X16641334>.
- Pereira, Gabriel, and Christoph Raetzsch. "From Banal Surveillance to Function Creep: Automated License Plate Recognition (ALPR) in Denmark." *Surveillance & Society* 20, no. 3 (2022): 265–80. <https://doi.org/10.24908/ss.v20i3.15000>.
- Plate Recognizer* (blog). "ANPR for UK." May 3, 2022. <https://platerecognizer.com/anpr-for-uk/>.
- Prasad, Ajay, Kaushik Ghosh, and Sourabh Singh Verma. "Crime Patrolling Assistance Using Passive Monitoring: A Proof of Concept of a Proactive Wi-Fi Surveillance System." In *Proceedings of the 12th International Conference on Computing Communication and Networking Technologies*, 1–11. Piscataway, NJ: IEEE, 2021. <https://doi.org/10.1109/ICCCNT51525.2021.9579805>.
- Rigano, Christopher. *Using Artificial Intelligence to Address Criminal Justice Needs*. Washington, DC: National Institute of Justice, 2018. <https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs>.
- Roberts, David J., and Meghann Casanova. *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement*. Alexandria, VA: International Association of Chiefs of Police, 2012. <https://trid.trb.org/view/1223372>.
- Rubel, Alan, Clinton Castro, and Adam Pham. *Algorithms and Autonomy: The Ethics of Automated Decision Systems*. Cambridge: Cambridge University Press, 2021. <https://doi.org/10.1017/9781108895057>.
- Schlabach, Gabriel R. "Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act." *Stanford Law Review* 67, no. 3 (March 2015): 677–721. <https://www.jstor.org/stable/43920972>.
- Sen, Sankar. *Enforcing Police Accountability through Civilian Oversight*. New Delhi: SAGE Publications, 2010.
- Sisson, Patrick. "In (and above) Beverly Hills, Police Are Watching." Bloomberg, January 19, 2023. <https://www.bloomberg.com/news/features/2023-01-19/in-beverly-hills-police-surveillance-technology-takes-off>.

- Slobogin, Christopher, and Sarah Brayne. "Surveillance Technologies and Constitutional Law." *Annual Review of Criminology* 6, no. 1 (2023): 219–40. <https://doi.org/10.1146/annurev-criminol-030421-035102>.
- Stone, Christopher, Todd Foglesong, and Christine M. Cole. *Policing Los Angeles under a Consent Decree: The Dynamics of Change at the LAPD*. Cambridge, MA: Harvard Kennedy School, 2009. <https://www.hks.harvard.edu/publications/policing-los-angeles-under-consent-decree-dynamics-change-lapd>.
- Stone, Christopher E., and Heather H. Ward. "Democratic Policing: A Framework for Action." *Policing and Society* 10, no. 1 (2000): 11–45. <https://doi.org/10.1080/10439463.2000.9964829>.
- Thomson, Jonny. "Algocracy Would Replace Politicians with Algorithms. Should We Try It?" Big Think, November 28, 2022. <https://bigthink.com/thinking/algocracy-algorithm-government/>.
- UK Government Digital Service. "Data Protection." Accessed April 16, 2023. <https://www.gov.uk/data-protection>.
- UK Information Commissioner's Office. "CCTV and Video Surveillance." Accessed February 27, 2023. <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv/>.
- . "What Is a DPIA?" Accessed July 21, 2023. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/>.
- Waldman, Ari, and Kirsten Martin. "Governing Algorithmic Decisions: The Role of Decision Importance and Governance on Perceived Legitimacy of Algorithmic Decisions." *Big Data & Society* 9, no. 1 (January 2022): 1–16. <https://doi.org/10.1177/20539517221100449>.
- Warren, Ian, Randy Lippert, Kevin Walby, and Darren Palmer. "When the Profile Becomes the Population: Examining Privacy Governance and Road Traffic Surveillance in Canada and Australia." *Current Issues in Criminal Justice* 25, no. 2 (November 2013): 565–84. <https://doi.org/10.1080/10345329.2013.12035984>.
- Wesner, Kearston, and Katie Blevins. "Restraining the Surveillance Society: Comparing Privacy Policies for Automated License Plate Readers in the United States and the United Kingdom." *Ohio State Technology Law Journal* 18, no. 1 (2021): 99–156. <http://hdl.handle.net/1811/101513>.
- Whittaker, Zack. "Police License Plate Readers Are Still Exposed on the Internet." TechCrunch, January 22, 2019. <https://techcrunch.com/2019/01/22/police-alpr-license-plate-readers-accessible-internet/>.

Willis, James J., Christopher Koper, and Cynthia Lum. "The Adaptation of License-Plate Readers for Investigative Purposes: Police Technology and Innovation Re-invention." *Justice Quarterly* 35, no. 4 (June 2018): 614–38. <https://doi.org/10.1080/07418825.2017.1329936>.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Fort Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California



DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE