

MARYLAND LAW REVIEW

VOLUME 74

2014

NUMBER 1

Articles

IMMIGRATION SURVEILLANCE

ANIL KALHAN*

ABSTRACT

In recent years, immigration enforcement levels have soared, yielding a widely noted increase in the number of noncitizens removed from the United States. Less visible, however, has been an attendant sea change in the underlying nature of immigration governance itself, hastened by new surveillance and dataveillance technologies. Like many other areas of contemporary governance, immigration control has rapidly become an information-centered and technology-driven enterprise. At virtually every stage of the

© 2014 Anil Kalhan

* Associate Professor of Law, Drexel University. A.B., Brown University; M.P.P.M., Yale School of Management; J.D., Yale Law School. Many thanks to Tabatha Abu El-Haj, Amna Akbar, Raquel Aldana, Efrat Arbel, Sameer Ashar, Stacy Caplow, Jennifer Chacón, Janie Chuang, Jennifer Daskal, Ingrid Eagly, Richard Frankel, Alex Geisinger, David Harris, Ernesto Hernández-López, Alan Hyde, Joy Kanwar, Sonia Katyal, Lisa Kerr, Jennifer Lee Koh, Joe Landau, Anna Law, Nancy Leong, Catherine MacAuliff, Koren Manning, Cyrus Mehta, Fernanda Nicola, Leslie Paik, Alison Parker, Frank Pasquale, Jayesh Rathod, Dana Remus, Pam Saunders, Collin Schueler, Mimi Sheller, Jayashri Srikantiah, Juliet Stumpf, Margaret Taylor, Katie Tinto, Tara Urs, and Jon Weinberg for valuable exchanges on the issues in this Article and helpful comments on earlier drafts, and to presentation attendees at American University Washington College of Law, Brooklyn Law School, University of Pittsburgh Law School, and the Immigration Law Teachers Workshop at UC Irvine School of Law for feedback on this project. I am also very thankful to Hillary Anderson for excellent research assistance, to Sunita Balija and John Cannan for very helpful research and library support, and to Liz Clark Rinehart, Susan Schipper, and the staff of the *Maryland Law Review* for helpful comments and outstanding editorial work. Finally, I am very thankful to Dean Roger Dennis for his support for this project.

process of migrating or traveling to, from, and within the United States, both noncitizens and U.S. citizens are now subject to collection and analysis of extensive quantities of personal information for immigration control and other purposes. This information is aggregated and stored by government agencies for long retention periods in networks of interoperable databases and shared among a variety of public and private actors, both inside and outside the United States, with little transparency, oversight, or accountability.

In this Article, I theorize and assess this underappreciated transformation of the techniques and technologies of immigration enforcement—their swift proliferation, enormous scale, likely entrenchment, and broader meanings. Situating this reconfiguration within a larger set of developments concerning surveillance and technology, I explain how these technologies have transformed a regime of immigration control, operating primarily upon noncitizens at the territorial border, into part of a more expansive regime of migration and mobility surveillance, operating without geographic bounds upon citizens and noncitizens alike. The technologies that enable this immigration surveillance regime can, and do, bring great benefits. However, their unimpeded expansion erodes the practical mechanisms and legal principles that have traditionally constrained aggregations of power and protected individual autonomy, as similarly illustrated in current debates over surveillance in other settings. In the immigration context, those constraints have always been less robust in the first place. Accordingly, I urge more constrained implementation of these technologies to preserve zones where immigration surveillance activities do not take place and to ensure greater due process and accountability when they do.

A complete understanding of immigration enforcement today must account for how the evolution of enforcement institutions, practices, and meanings has not simply increased the number of noncitizens being deported but has effected a more basic transformation in immigration governance. The institutions of immigration surveillance are becoming integrated into the broader national surveillance state very rapidly. As that reconfiguration proceeds, scholars, policymakers, advocates, and community members need to grapple more directly with its implications.

TABLE OF CONTENTS

ABSTRACT..... 1

TABLE OF CONTENTS 3

INTRODUCTION..... 4

I. THE TRANSFORMATION OF IMMIGRATION ENFORCEMENT 11

 A. Monitoring and Regulating Entry 13

 B. Direct Post-Entry Monitoring and Enforcement 19

 C. Indirect Post-Entry Monitoring and Enforcement..... 25

 D. Criminal Prosecution of Migration-Related Offenses 27

 E. Exit Controls 29

II. THE NEW SURVEILLANCE INFRASTRUCTURE OF MASS IMMIGRATION ENFORCEMENT 30

 A. The Functions and Practices of Immigration Surveillance..... 31

 1. Identification 31

 2. Analysis, Screening, and Authorization 35

 3. Mobility Tracking and Control..... 40

 4. Information Sharing and Interoperability..... 43

 B. Immigration Enforcement as Immigration Surveillance 45

 1. Border Control 46

 2. Overseas Visa Issuance and Refugee Processing 47

 3. Entry, Exit, and Travel Control 48

 4. Post-Entry Enforcement..... 52

III. LEGALIZATION AND THE IMMIGRATION SURVEILLANCE STATE ... 59

IV. THE CONSEQUENCES OF IMMIGRATION SURVEILLANCE 64

 A. Deterritorializing the Migration Border 65

 B. Automating the Migration Border..... 70

 C. Data Collection, Retention, and Secondary Use 77

V. CONSTRAINING THE IMMIGRATION SURVEILLANCE STATE..... 80

 A. Protecting Information Interests in Migration, Mobility, and Travel..... 80

 B. Ending Border and Immigration Exceptionalism 82

 C. Transparency, Oversight, and Due Process 84

VI. CONCLUSION 86

INTRODUCTION

In recent years, the politics of immigration have been in a state of considerable flux. Although only months before the 2012 election the Republican Party and its presidential nominee officially embraced policies aimed at inducing large-scale “self-deportation” by unauthorized migrants, in the wake of the election leading Republicans exhibited a widely noted change of heart, facilitating the Senate’s bipartisan adoption of sweeping comprehensive immigration reform legislation.¹ Since then, legislative reform efforts in Congress have stalled, leaving the prospects for significant immigration reform legislation deeply uncertain.

However, even if Congress eventually embraces comprehensive immigration reform, the sprawling immigration enforcement system that has emerged in recent decades appears certain not just to endure, but to extend its reach. The reform frameworks advanced by the Obama Administration and leading members of Congress, while committing to legalize millions of unauthorized migrants, all pledge major expansions in border security and immigration control.² Although the particular forms of regulation remain in flux, any reforms that occur undoubtedly will include an aggressive, continuing commitment to large-scale enforcement measures.³

In this Article, I examine a set of important but underappreciated consequences of this entrenchment of mass immigration enforcement, tracing and analyzing the evolution of

1. Ryan Lizza, *Getting to Maybe: Inside the Gang of Eight’s Immigration Deal*, NEW YORKER, Jun. 24, 2013, at 44; see Anil Kalhan, *The Fourth Amendment and Privacy Implications of Interior Immigration Enforcement*, 41 U.C. DAVIS L. REV. 1137, 1165–67 (2008) (discussing “self-deportation”).

2. Border Security, Economic Opportunity, and Immigration Modernization Act, S. 744, 113th Cong. (as passed by Senate, June 27, 2013); *Fact Sheet: Fixing Our Broken Immigration System So Everyone Plays by the Rules*, WHITE HOUSE (Jan. 29, 2013), <http://www.whitehouse.gov/the-press-office/2013/01/29/fact-sheet-fixing-our-broken-immigration-system-so-everyone-plays-rules>; *Text of Republicans’ Principles on Immigration*, N.Y. TIMES (Jan. 31, 2014), <http://nyti.ms/1a4AeTh>.

3. See, e.g., Marco Rubio, *Mis Principios Para Una Reforma Migratoria*, LA OPINIÓN (Jan. 23, 2013), <http://www.laopinion.com/marco-rubio-principios-reforma-migratoria> (advocating enforcement “triggers” as precondition to legalization of unauthorized migrants); Seth Freed Wessler, *How Immigration Reform Could Expand Incarceration of Immigrants*, COLORLINES (Feb. 6, 2013), http://colorlines.com/archives/2013/02/how_immigration_reform_could_mean_more_incarceration_of_immigrants.html; see also David A. Martin, *Eight Myths About Immigration Enforcement*, 10 N.Y.U. J. LEGIS. & PUB. POL’Y 525, 526 (2007) (advocating a “stable, enduring, and functional enforcement system” as an “indispensable component of viable immigration reform”).

immigration governance into an enduring regime of *immigration surveillance*.⁴ By any measure, enforcement levels have soared in recent years. Federal expenditures on border and immigration control have grown fifteen-fold since 1986 and now substantially exceed expenditures on all other federal law enforcement programs combined.⁵ These activities have been supplemented by a dizzying array of initiatives, often administered by state, local, and private actors, that indirectly enforce immigration law by regulating access to rights, benefits, and services—including employment, social services, driver’s licenses, transportation services, and education—based on citizenship or immigration status.⁶ Increasingly, immigration control objectives also are pursued using criminal prosecutions.⁷

These initiatives have yielded a staggering, widely noted increase in the number of noncitizens formally removed from the United States.⁸ Much less widely noted, however, has been the full

4. JOHN GILLIOM & TORIN MONAHAN, SUPERVISION: AN INTRODUCTION TO THE SURVEILLANCE SOCIETY 2 (2013) (defining surveillance as involving “systematic monitoring, gathering, and analysis of information in order to make decisions, minimize risk, sort populations, and exercise power”); DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 14 (2007); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008); Gary T. Marx, *What’s New About the “New Surveillance”?* *Classifying for Change and Continuity*, 1 SURVEILLANCE & SOC’Y 9, 18 (2002).

5. DORIS MEISSNER, DONALD M. KERWIN, MUZAFFAR CHISHTI & CLAIRE BERGERON, MIGRATION POL’Y INST., IMMIGRATION ENFORCEMENT IN THE UNITED STATES: THE RISE OF A FORMIDABLE MACHINERY (2013). The federal judiciary has also devoted a growing share of its resources to adjudicating immigration enforcement cases. ABA COMM’N ON IMMIGRATION, REFORMING THE IMMIGRATION SYSTEM: PROPOSALS TO PROMOTE INDEPENDENCE, FAIRNESS, EFFICIENCY, AND PROFESSIONALISM IN THE ADJUDICATION OF REMOVAL CASES 1-33 & n.242, 3-21 to 3-26 (2010).

6. Monica Varsanyi, *Immigration Policy Activism in U.S. States and Cities: Interdisciplinary Perspectives*, in TAKING LOCAL CONTROL: IMMIGRATION POLICY ACTIVISM IN U.S. CITIES AND STATES 1, 3 (Monica Varsanyi ed., 2010); Michael J. Wishnie, *Prohibiting the Employment of Unauthorized Immigrants: The Experiment Fails*, 2007 U. CHI. LEGAL F. 193 (2007); see Kalhan, *supra* note 1, at 1158–60 (conceptualizing the distinction between direct and indirect enforcement mechanisms).

7. Jennifer M. Chacón, *Managing Migration Through Crime*, 109 COLUM. L. REV. SIDEBAR 135 (2009); Ingrid V. Eagly, *Prosecuting Immigration*, 104 NW. U. L. REV. 1281 (2010); David Sklansky, *Crime, Immigration, and Ad Hoc Instrumentalism*, 15 NEW CRIM. L. REV. 157 (2012).

8. MARC R. ROSENBLUM, DORIS MEISSNER, CLAIRE BERGERON & FAYE HIPSMAN, MIGRATION POL’Y INST., THE DEPORTATION DILEMMA: RECONCILING TOUGH AND HUMANE ENFORCEMENT 3–6 (2014); *Developments in the Law—Immigrants Rights & Immigration Enforcement*, 126 HARV. L. REV. 1565, 1569–70 (2013); *The Great Expulsion*, ECONOMIST, Feb. 8, 2014, at 23; Adam Goodman, *How the Deportation Numbers Mislead*, ALJAZEERA AM. (Jan. 24, 2014), <http://alj.am/1avrZQT>. From 1986 to 2012, the annual number of formal removals skyrocketed from approximately 25,000 to over 419,000 individuals. DEP’T OF HOMELAND SEC., OFFICE OF IMMIGR. STATS., IMMIGRATION ENFORCEMENT ACTIONS: 2012 (2013). Hundreds of thousands of noncitizens are detained each year while in removal

significance of that growth—including an attendant sea change in the underlying nature of immigration regulation itself, hastened by the implementation of transformative new surveillance and dataveillance technologies. Like many other areas of contemporary governance, immigration control has rapidly become an information-centered and technology-driven enterprise. At virtually every stage of the process of migrating or traveling to, from, and within the United States, both noncitizens and U.S. citizens are now subject to collection and analysis of extensive quantities of personal information for immigration control and other purposes. This information is aggregated and stored by government agencies for long retention periods in networks of interoperable databases and shared among a variety of public and private actors, both inside and outside the United States, with little transparency, oversight, or accountability.⁹

Despite the growing concern about surveillance and data mining in other contexts, the development of this immigration surveillance regime has received limited attention.¹⁰ Although a rich literature assesses shifts in immigration law in recent decades, the transformation of enforcement practices themselves—understood as a conceptual and programmatic whole, rather than a series of discrete programs—remains insufficiently examined.¹¹ When analyzing

proceedings or awaiting removal. Anil Kalhan, *Rethinking Immigration Detention*, 110 COLUM. L. REV. SIDEBAR 42, 44–45 (2010). Federal convictions for migration-related crimes have also spiraled upward, from approximately 9,000 in 1986 to over 27,000 by 2010. U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS, IMMIGRATION OFFENDERS IN THE FEDERAL JUSTICE SYSTEM, 2010 (2012). While more uneven, workplace enforcement of laws barring employment of unauthorized workers also has increased. ANDORRA BRUNO, CONG. RESEARCH SERV., IMMIGRATION-RELATED WORKSITE ENFORCEMENT: PERFORMANCE MEASURES 5–13 (2012).

9. MEISSNER ET AL., *supra* note 5, at 66 (“Database screening now accompanies virtually all key interactions between noncitizens and the federal government.”); Anil Kalhan, *Immigration Policing and Federalism Through the Lens of Technology, Surveillance, and Privacy*, 74 OHIO ST. L.J. 1105 (2013); Valsamis Mitsilegas, *Extraterritorial Immigration Control in the 21st Century: The Individual and the State Transformed*, in EXTRATERRITORIAL IMMIGRATION CONTROL: LEGAL CHALLENGES 39, 39 (Bernard Ryan & Valsamis Mitsilegas eds., 2010); Tamara Vukov & Mimi Sheller, *Border Work: Surveillance, Virtual Fences, and Tactical Counter-Media*, 23 SOC. SEMIOTICS 225 (2013).

10. MEISSNER ET AL., *supra* note 5, at 65 (noting that these technologies have been “transformational” but “ha[ve] not received the attention given to more visible changes”).

11. See Hiroshi Motomura, *Choosing Immigrants, Making Citizens*, 59 STAN. L. REV. 857, 870 (2007) (emphasizing the need to “think systematically about . . . immigration law choices”); Cristina M. Rodríguez, *The Integrated Regime of Immigration Regulation*, in WRITING IMMIGRATION: SCHOLARS AND JOURNALISTS IN DIALOGUE 44 (Marcelo Suárez-Orozco, Vivian Louie, & Roberto Suro eds., 2011) (urging integrated analysis of the “federal-state-local dynamic in immigration regulation” as a coherent whole); Mariano-Florentino Cuellar,

enforcement in systemic terms, scholars have emphasized other important concerns, such as the meaning and significance of deportation and unlawful presence.¹² Observers have carefully examined immigration law's adjudicatory processes and its convergence with criminal law norms and practices.¹³ Scholars also have addressed the significance of race, religion, national origin, gender, sexual orientation, and class in enforcement practices.¹⁴ And a growing body of work explores immigration federalism and localism.¹⁵

The Political Economies of Immigration Law, 2 UC IRVINE L. REV. 1 (2012) (highlighting broad areas of convergence among seemingly disparate immigration-related issues).

12. See, e.g., BILL ONG HING, *DEPORTING OUR SOULS: VALUES, MORALITY, AND IMMIGRATION POLICY* (2006); DANIEL KANSTROOM, *AFTERMATH: DEPORTATION LAW AND THE NEW AMERICAN DIASPORA* (2012); HIROSHI MOTOMURA, *IMMIGRATION OUTSIDE THE LAW* (2014); Stephen Legomsky, *Immigration Policy from Scratch: The Universal and the Unique*, 21 WM. & MARY BILL RTS. J. 339 (2012); Alexandra Natapoff, *Underenforcement*, 75 FORDHAM L. REV. 1715, 1735–39 (2006); Michael J. Wishnie, *Proportionality: The Struggle for Balance in U.S. Immigration Policy*, 72 U. PITT. L. REV. 431 (2011).

13. See, e.g., Jennifer M. Chacón, *Overcriminalizing Immigration*, 102 J. CRIM. L. & CRIMINOLOGY 613 (2012); Jill E. Family, *A Broader View of the Immigration Adjudication Problem*, 23 GEO. IMMIGR. L.J. 595 (2009); Stephen H. Legomsky, *The New Path of Immigration Law: Asymmetric Incorporation of Criminal Justice Norms*, 64 WASH. & LEE L. REV. 469 (2007); Teresa A. Miller, *Citizenship and Severity: Recent Immigration Reforms and the New Penology*, 17 GEO. IMMIGR. L.J. 611 (2003); Nancy Morawetz, *Understanding the Impact of the 1996 Deportation Laws and the Limited Scope of Proposed Reforms*, 113 HARV. L. REV. 1936 (2000); Juliet P. Stumpf, *The Crimmigration Crisis: Immigrants, Crime, and Sovereign Power*, 56 AM. U. L. REV. 367 (2006).

14. E.g., Susan M. Akram & Kevin R. Johnson, *Race, Civil Rights, and Immigration Law After September 11, 2001: The Targeting of Arabs and Muslims*, 58 N.Y.U. ANN. SURV. AM. L. 295 (2002); Raquel Aldana, *Of Katz and "Aliens": Privacy Expectations and the Immigration Raids*, 41 U.C. DAVIS L. REV. 1081 (2008); Devon W. Carbado & Cheryl I. Harris, *Undocumented Criminal Procedure*, 58 UCLA L. REV. 1543 (2011); Jennifer Gordon & R.A. Lenhardt, *Citizenship Talk: Bridging the Gap Between Immigration and Race Perspectives*, 75 FORDHAM L. REV. 2493 (2007); Kevin R. Johnson, *The Intersection of Race and Class in U.S. Immigration Law and Enforcement*, 72 LAW & CONTEMP. PROBS. 1 (2009); Jayashri Srikantiah, *Perfect Victims and Real Survivors: The Iconic Victim in Domestic Human Trafficking Law*, 87 B.U. L. REV. 157 (2007); SHARITA GRUBERG, *CTR. FOR AM. PROGRESS, DIGNITY DENIED: LGBT IMMIGRANTS IN U.S. IMMIGRATION DETENTION* (2013).

15. E.g., Jennifer M. Chacón, *The Transformation of Immigration Federalism*, 21 WM. & MARY BILL RTS. J. 577 (2012); Stella Burch Elias, *The New Immigration Federalism*, 74 OHIO ST. L.J. 703 (2013); Lucas Guttentag, *Discrimination, Preemption, and Arizona's Immigration Law: A Broader View*, 65 STAN. L. REV. ONLINE 1 (2012); Clare Huntington, *The Constitutional Dimension of Immigration Federalism*, 61 VAND. L. REV. 787 (2008); Anil Kalhan, *Immigration Enforcement and Federalism After September 11, 2001*, in *IMMIGRATION, INTEGRATION, AND SECURITY: AMERICA AND EUROPE IN COMPARATIVE PERSPECTIVE* (Ariane Chebel d'Appollonia & Simon Reich eds., 2008); Hiroshi Motomura, *The Discretion That Matters: Federal Immigration Enforcement, State and Local Arrests, and the Civil-Criminal Line*, 58 UCLA L. REV. 1819 (2011); Cristina M. Rodríguez, *The Significance of the Local in Immigration Regulation*, 106 MICH. L. REV. 567 (2008); Peter H. Schuck, *Taking Immigration Federalism Seriously*, 2007 U. CHI. LEGAL F. 57 (2007).

However, legal scholars have given virtually no attention to the revolution taking place in the techniques and technologies of immigration enforcement themselves—their swift proliferation, enormous scale, likely entrenchment, and broader meanings. In this Article, I theorize and assess these shifts, situating and analyzing them within a broader, longer term set of developments concerning technology and surveillance in contemporary governance.¹⁶ Immigration control has not simply evolved into a system to effectuate the removal of noncitizens on a massive scale, although it manifestly has done that. More fundamentally, the evolution of this system has reshaped the meanings and functions of immigration governance itself, transforming a regime of immigration control, operating primarily upon noncitizens at the border, into part of a more expansive regime of migration and mobility surveillance, operating without geographic bounds upon citizens and noncitizens alike.¹⁷ Traditional immigration law frameworks offer neither the vocabulary to fully engage with this transformation nor the mechanisms to constrain these surveillance activities across the many domains in which they occur. Accordingly, I advance a framework to understand and respond to these developments rooted in scholarship on surveillance and privacy, bridging a larger divide identified by Vicki Squire between scholarship on the law and politics of “control” and scholarship on the law and politics of “migration or movement.”¹⁸

After recounting and interpreting the immigration enforcement system’s rapid expansion and reconfiguration in Part I, I demonstrate in Part II how new technologies have reconfigured approaches to four distinct sets of immigration surveillance practices: *identification*, *screening and authorization*, *mobility tracking and control*, and *information sharing*. These systems and processes routinize the collection, storage,

16. See GILLIOM & MONAHAN, *supra* note 4; Balkin, *supra* note 4; Marx, *supra* note 4; see also Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 101, 106 (2008) (discussing implications of the emergence of “nonphysical, technology-based means of control,” such as location tracking, biometric scanning, and electronic indexing, in criminal justice processes).

17. Cf. DAVID GARLAND, *THE CULTURE OF CONTROL: CRIME AND SOCIAL ORDER IN CONTEMPORARY SOCIETY* 168 (2001) (explaining the process by which the “institutional architecture” and “state apparatus” of criminal justice have remained “firmly in place,” but have been transformed in their “deployment, strategic functioning, and social significance”); SASKIA SASSEN, *TERRITORY, AUTHORITY, RIGHTS: FROM MEDIEVAL TO GLOBAL ASSEMBLAGES* 1, 403 (2006) (discussing “micro-processes” of globalization that “begin to denationalize what had been constructed as national”).

18. Vicki Squire, *The Contested Politics of Mobility in THE CONTESTED POLITICS OF MOBILITY: BORDERZONES AND IRREGULARITY* 1, 3–4 (Vicki Squire ed. 2011); see Murphy, *supra* note 16 (bridging the analogous divide between scholarship on criminal incapacitation and scholarship on privacy and surveillance).

aggregation, processing, and dissemination of detailed personal information for immigration control and other purposes on an unprecedented scale and facilitate the involvement of an escalating number of federal, state, local, private, and non-U.S. actors in immigration control activities. In Part III, I explain why the legalization provisions in comprehensive immigration reform proposals would only make this emergent surveillance regime more durable and pervasive, since the logic of surveillance—and of making unauthorized migrants legible and visible to the state—is embedded within those legalization proposals themselves. This consistency between the rationales for legalization and immigration surveillance also can be seen in the Obama Administration’s Deferred Action for Childhood Arrivals (“DACA”) program, which illustrates on a smaller scale what immigration surveillance could look like in the context of any large scale legalization program that Congress might choose to adopt.

In the remainder of the Article, I consider the implications of this reordering. In Part IV, I situate immigration surveillance within broader developments concerning technology, surveillance, and privacy, analyzing the consequences of routinized and widening collection, processing, retention, and dissemination of detailed personal information for immigration control purposes. As these immigration surveillance activities have proliferated, what I term the *migration border*—the set of boundary points at which nation-states authorize individuals to enter or be admitted, prevent or allow their entry or admission, or subject them to possible expulsion—has been decoupled from the territorial border and rendered “virtual”: layered, electronic, mobile, and policed by an escalating number of public and private actors. In the process, the lines between immigration control and other regulatory domains have blurred.

The technologies that enable immigration surveillance are not inherently harmful; indeed, many of them can and do bring significant benefits. However, their unconstrained implementation also carries several categories of underappreciated costs—all of which are exacerbated by the extent of deference afforded in the context of immigration enforcement, border control, and national security. Accordingly, in Part V, I identify and advance principles to constrain, inform, and guide the implementation of these tools of the “automated administrative state.”¹⁹ As illustrated in current debates

19. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1258 (2008); see also Kalhan, *supra* note 9.

over surveillance and data mining by the National Security Agency and other institutions, both public and private, the unimpeded expansion of surveillance and dataveillance mechanisms erodes both the legal principles and the practical mechanisms that have traditionally constrained aggregations of public and private power and protected individual autonomy and privacy.²⁰ In the immigration context, those constraints have always been less robust than in many other regulatory domains. Drawing upon surveillance and privacy scholarship, I urge more constrained implementation of these powerful technologies, with greater transparency and oversight, to preserve zones where immigration surveillance activities do not take place and to ensure greater due process and accountability when they do.

A complete understanding of immigration regulation today must account for how the evolution of enforcement institutions, practices, and meanings has not simply increased the number of noncitizens being deported, but has effected a more basic transformation in immigration governance, in a manner that experiences outside the immigration context similarly illustrate.²¹ Nor is the onset of the immigration surveillance state solely of concern to immigration specialists, especially since experience shows that innovations in surveillance techniques and technologies often are initiated with groups that are vulnerable or subject to heightened control—

20. GLENN GREENWALD, *NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE* (2014); SIVA VAIDHYANATHAN, *THE GOOGLIZATION OF EVERYTHING (AND WHY WE SHOULD WORRY)* (2011); Alice E. Marwick, *How Your Data Are Being Deeply Mined*, N.Y. REV. BOOKS, Jan. 9, 2014, at 22.

21. GARY T. MARX, *UNDERCOVER: POLICE SURVEILLANCE IN AMERICA* 208 (1988) (“Computers qualitatively alter the nature of surveillance—routinizing, broadening, and deepening it”); Bernard E. Harcourt, *After the “Social Meaning Turn”: Implications for Research Design and Methods of Proof in Contemporary Criminal Law Policy Analysis*, 34 *LAW & SOC’Y REV.* 179, 182 (2000) (arguing that curfew laws and order maintenance policing not only “influence . . . short-term behavior” as intended but also “reconfigure” and “more deeply affect our very understanding of order or disorder” and “shape us as contemporary subjects of society”); MARIANO-FLORENTINO CUÉLLAR, *GOVERNING SECURITY: THE HIDDEN ORIGINS OF AMERICAN SECURITY AGENCIES* xi–xii (2013) (arguing that interplay between “architecture of public agencies . . . political strategies, and legal interpretations” has “shaped public perceptions of [national] security” and “given life” to its meaning); GARLAND, *supra* note 17, at 194 (arguing that crime control strategies have not simply been responses to “political and cultural values” of “the late modern world,” but have “play[ed] a role in *creating* that world, helping to constitute the meaning of late modernity”); DIANE RAVITCH, *THE DEATH AND LIFE OF THE GREAT AMERICAN SCHOOL SYSTEM* (2010) (arguing that emphasis on accountability and testing in education reform has reshaped the nature and meaning of education itself).

including noncitizens—before later going mainstream.²² As the institutions of immigration surveillance rapidly become integrated into the broader national surveillance state, the need to squarely address the consequences of that reconfiguration becomes more acute.²³

I. THE TRANSFORMATION OF IMMIGRATION ENFORCEMENT

Before assessing the shifts currently taking place in the nature of immigration governance with the implementation of new technologies, it is necessary to first understand the development and proliferation of the immigration enforcement activities into which these new systems are being deployed. While regularized enforcement programs were limited for much of U.S. history and have tended to emphasize control of the territorial border with Mexico, in recent decades immigration monitoring and control initiatives have grown explosively across a much broader range of domains.²⁴ In this Part, to establish the context for the technology-enabled shifts that I examine in this Article, I recount this transformation, which spans every stage of the migration process: before individuals travel to the United States, during their travel and when they seek to enter, while they are present, and when they depart. I identify and discuss major shifts in the modalities and

22. SIMON A. COLE, *SUSPECT IDENTITIES: A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION* 119–20 (2001) (explaining that late 19th century innovations in fingerprint identification were “stimulated by a perceived need to identify ‘faceless,’ racially unfamiliar” recent immigrants); GILLIOM & MONAHAN, *supra* note 4, at 73 (describing schools, prisons, and military institutions as “laboratories for new surveillance practices” in which “innovations in surveillance technology are first deployed”); Virginia Eubanks, *Want to Predict the Future of Surveillance? Ask Poor Communities*, AM. PROSPECT (Jan. 15, 2014), <http://prospect.org/article/want-predict-future-surveillance-ask-poor-communities>; see David Cole, *Enemy Aliens*, 54 STAN. L. REV. 953, 959 (2002) (“[W]hat we are willing to allow our government to do to immigrants creates precedents for how it treats citizens.”).

23. Balkin, *supra* note 4; Gus Hosein, *Defining the Surveillance State*, PRIVACY INT’L (Oct. 31, 2013), <http://www.privacyinternational.org/blog/defining-the-surveillance-state>; see also GILLIOM & MONAHAN, *supra* note 4, at 45 (describing the process by which “all significant institutions are implementing similar models of governance” that “use[] identification, visibility, and surveillance as [their] central strategies”).

24. PETER ANDREAS, *BORDER GAMES: POLICING THE U.S.-MEXICO DIVIDE* 88 (2000); BILL ONG HING, *DEFINING AMERICA THROUGH IMMIGRATION POLICY* 115 (2004); DANIEL KANSTROOM, *DEPORTATION NATION: OUTSIDERS IN AMERICAN HISTORY* 2, 6 (2007) (characterizing the deportation system as having grown “slowly, incrementally, and reactively” from “decentralized” and “inefficient” beginnings); DOUGLAS S. MASSEY, JORGE DURAND & NOLAN J. MALONE, *BEYOND SMOKE AND MIRRORS: MEXICAN IMMIGRATION IN AN ERA OF ECONOMIC INTEGRATION* 26 (2003) (describing early border control efforts as “more symbolic than real”); MAE M. NGAI, *IMPOSSIBLE SUBJECTS: ILLEGAL ALIENS & THE MAKING OF MODERN AMERICA* (2004); Gerald L. Neuman, *The Lost Century of American Immigration Law (1776-1875)*, 93 COLUM. L. REV. 1833 (1993).

priorities of enforcement across five categories: (1) initiatives that monitor and regulate entry into the United States, (2) post-entry initiatives that directly monitor and regulate noncitizens, (3) post-entry initiatives that indirectly monitor and regulate noncitizens, (4) criminal prosecutions, and (5) initiatives that monitor and regulate departures from the United States.

Importantly, while these programs have been initiated and implemented as immigration control measures, many of these measures necessarily operate upon and are experienced by both noncitizens and U.S. citizens alike.²⁵ Increasingly, many of these initiatives also are being deployed to serve a range of other, non-immigration-related purposes. For example, especially in the aftermath of the 2001 terrorist attacks and the creation of the Department of Homeland Security (“DHS”), immigration enforcement activities have increasingly been cast with security-related significance.²⁶ In 2003, the immigration-related functions formerly performed by the Immigration and Naturalization Service (“INS”), within the Department of Justice, were transferred to three new agencies with DHS: U.S. Customs and Border Protection (“CBP”), U.S. Citizenship and Immigration Services (“USCIS”), and U.S. Immigration and Customs Enforcement (“ICE”)—all of which are charged to approach immigration governance first and foremost through the lens of security.²⁷ Paradoxically, even as it has significantly intensified immigration enforcement activities, the United States has continued to encourage expanded migration flows while simultaneously seeking to control the nature and patterns of those flows. As a result, the expansion of immigration enforcement measures discussed in this Part has operated not only to facilitate the expulsion of potentially removable noncitizens, as discussions of immigration enforcement usually emphasize, but also to enable additional forms of regulation, control, and exclusion that are experienced by both noncitizens and citizens.²⁸

25. Kalhan, *supra* note 1, at 1149.

26. CUÉLLAR, *supra* note 21, at 125–89.

27. See MICHELLE MITTELSTADT, BURKE SPEAKER, DORIS MEISSNER & MUZAFFAR CHISHTI, MIGRATION POL’Y INST., THROUGH THE PRISM OF NATIONAL SECURITY: MAJOR IMMIGRATION POLICY AND PROGRAM CHANGES IN THE DECADE SINCE 9/11 (2011).

28. See PHILIP KRETSEDEMAS, MIGRANTS AND RACE IN THE US: TERRITORIAL RACISM AND THE ALIEN OUTSIDE 39, 122 (2013) (observing that the “practical effect” of expanded immigration enforcement “has been to control an expanding migrant flow and not to reduce the number of migrants entering the nation”); Philip Kretsedemas, *The Limits of Control: Neo-Liberal Policy Priorities and the U.S. Non-Immigrant Flow*, 50 INT’L MIGRATION e1, e1 (2012) (analyzing the relationship between the “apparently divergent trends” of “liberali-

A. *Monitoring and Regulating Entry*

Historically, territorial borders and their functional equivalents have been the focal points of immigration control, and as immigration enforcement activities have expanded in recent decades, the federal government has continued to invest heavily in border control and other measures to control entry into the United States. Among these measures, the most visible initiative involves the quasi-militarized fortification of the U.S.-Mexico land border.²⁹ CBP's Border Patrol, which totaled a few thousand agents in the early 1990s, has doubled since 2004 to over 21,000 agents, with the vast majority posted along the southwestern border.³⁰ In addition, congressional mandates have prompted the construction of over 650 miles of fencing and other physical barriers.³¹ Current immigration reform proposals would go dramatically further, doubling both the number of Border Patrol agents and the extent of fencing and physical barriers.³²

Regulation of the U.S.-Canada border, by contrast, has historically been more limited, but since 2001, security-driven anxieties have effected a shift toward what Peter Andreas describes as

zation of migrant flows," on the one hand, and "the intensification of immigration enforcement," on the other); *see also* KUNAL M. PARKER, *IMMIGRANTS AND OTHER FOREIGNERS IN AMERICA: A HISTORY OF IMMIGRATION AND CITIZENSHIP LAW* (forthcoming 2015) (manuscript at 4) (explaining and documenting the ways in which U.S. immigration and citizenship law historically has encompassed "efforts to render [individuals] foreign that have applied to insiders *and* outsiders, neighbors *and* strangers," including U.S. citizens and noncitizens alike).

29. ANDREAS, *supra* note 24, at 85–112; MASSEY ET AL., *supra* note 24, at 96–98.

30. MARC R. ROSENBLUM, CONG. RESEARCH SERV., *BORDER SECURITY: IMMIGRATION ENFORCEMENT BETWEEN PORTS OF ENTRY* 14–15 (2013). The Obama Administration also has deployed approximately 1,200 National Guard personnel to support the Border Patrol along the southwestern border. MEISSNER ET AL., *supra* note 5, at 25–26.

31. Consolidated Appropriations Act of 2008 § 564, Pub. L. No. 110-161, 121 Stat. 2090, 2090–91 (2007); Secure Fence Act of 2006 § 3, Pub. L. No. 109-367, 120 Stat. 2638, 2638–39 (2006); REAL ID Act of 2005, Pub. L. No. 109-13, Div. B, 119 Stat. 302, 302–23 (2005); Illegal Immigration Reform and Immigrant Responsibility Act of 1996 § 102(a)–(c), Pub. L. No. 104-208, 110 Stat. 554, 554–55 (1996); *see* MEISSNER ET AL., *supra* note 5, at 30–31; Denise Gilman, *Seeking Breaches in the Wall: An International Human Rights Law Challenge to the Texas-Mexico Border Wall*, 46 TEX. INT'L L.J. 257, 258 (2011); Pratheepan Gulasekaram, *Why a Wall?*, 2 U.C. IRVINE L. REV. 147, 151 (2012).

32. Border Security, Economic Opportunity and Immigration Modernization Act, S. 744, 113th Cong. §§ 1101–1123 (as passed by Senate, June 27, 2013); *see also Fact Sheet, Emergency Supplemental Request to Address the Increase in Child and Adult Migration from Central America in the Rio Grande Valley Areas of the Southwest Border*, WHITE HOUSE (July 8, 2014), <http://www.whitehouse.gov/the-press-office/2014/07/08/fact-sheet-emergency-supplemental-request-address-increase-child-and-adu>.

the “Mexicanization” of the northern border.³³ The number of Border Patrol agents posted along the U.S.-Canada border has increased from a few hundred in the 1990s to over 2,200 today.³⁴ Since 2001, the United States, Canada, and Mexico have coordinated other enforcement practices. Border enforcement teams and security task forces have been established with both Canada and Mexico to coordinate investigations and other activities, and plans exist to expand this cooperation.³⁵ The United States and Canada also have entered into a “safe third country” agreement that largely bars refugee claimants arriving in one country from seeking protection in the other.³⁶

However, officials have gone well beyond these North America-specific initiatives, taking aggressive steps to regulate and monitor lawful entry into the United States more generally. These initiatives build on mechanisms that have long existed. For noncitizens, Congress has long required immigrant or nonimmigrant visas, with limited exceptions, before entering the United States and has established grounds of inadmissibility or excludability to screen out noncitizens deemed to raise public safety, public health, national security, and other social concerns.³⁷ While U.S. citizens are generally assumed to have a right to enter the United States—and at times have been subject to very minimal scrutiny when entering—U.S. officials

33. Peter Andreas, *The Mexicanization of the US-Canada Border: Asymmetric Interdependence in a Changing Security Context*, 60 INT’L J. 449 (2005); Audrey Macklin, *Disappearing Refugees: Reflections on the Canada-U.S. Safe Third Country Agreement*, 36 COLUM. HUM. RTS. L. REV. 365, 411 (2005).

34. MEISSNER ET AL., *supra* note 5, at 18, 38–39; Nina Bernstein, *Border Sweeps in North Reach Miles into U.S.*, N.Y. TIMES, Aug. 29, 2010, at A1.

35. Canada-U.S. Smart Border Declaration: Building a Smart Border for the 21st Century on the Foundation of a North American Zone of Confidence, Dec. 12, 2001; U.S.-Canada Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness, Dec. 2011; *see* CLARE RIBANDO SEELKE & KRISTIN M. FINKLEA, CONG. RESEARCH SERV., U.S.-MEXICAN SECURITY COOPERATION: THE MÉRIDA INITIATIVE AND BEYOND (2013); Sigrid Arzt, *U.S.-Mexico Security Collaboration: Intelligence Sharing and Law Enforcement Cooperation*, in SHARED RESPONSIBILITY: U.S.-MEXICO POLICY OPTIONS FOR CONFRONTING ORGANIZED CRIME 351 (Eric L. Olson, David A. Shirk & Andrew D. Selee eds., 2010); Kent Roach, *Uneasy Neighbors: Comparative American and Canadian Counter-Terrorism*, 38 WM. MITCHELL L. REV. 1701, 1790–94 (2012).

36. Safe Third Country Agreement, Can.-U.S., Dec. 5, 2002; Efrat Arbel, *Shifting Borders and the Boundaries of Rights: Examining the Safe Third Country Agreement Between Canada and the United States*, 25 INT’L J. REFUGEE L. 65 (2013).

37. IRA J. KURZBAN, IMMIGRATION LAW SOURCEBOOK 41–98 (13th ed. 2012). Under the Immigration and Nationality Act, a “nonimmigrant” is a noncitizen who falls within one of a variety of statutorily defined categories of non-permanent entrants to the United States. The statute defines all other noncitizens as “immigrants.” 8 U.S.C. § 1101(a)(15) (2013).

have nevertheless historically exercised control over international travel by U.S. citizens, including their entry in the United States, through the issuance, recognition, and revocation of U.S. passports and by other regulatory means.³⁸ Procedurally, when seeking to enter the United States, both noncitizens and U.S. citizens have traditionally been subject at the border to questioning and “routine” suspicionless searches and seizures, which the Supreme Court has deemed to be per se reasonable when conducted for purposes of enforcing immigration and customs laws—and therefore exempt from the Fourth Amendment’s warrant and probable cause requirements—“simply by virtue of the fact that they occur at the border.”³⁹

In recent years, however, efforts to control entry have extended well beyond traditional means of excluding noncitizens, regulating U.S. citizen travel, and conducting ordinary searches and seizures at the border, as both noncitizens and U.S. citizens have been subject to more intensive scrutiny at every stage of the process of migrating or traveling to the United States. Most of these new initiatives have roots in immigration policy debates that predate the 2001 terrorist attacks. For example, in the 1980s and 1990s, Congress steadily expanded the grounds upon which noncitizens may be barred from entry or admission and curtailed the opportunities for those grounds to be waived.⁴⁰ But as with the Canada-specific initiatives discussed above, efforts to tighten control over entry since 2001 increasingly have been justified with reference to national security and criminal law enforcement, and have emphasized the collection, storage,

38. *Nguyen v. Immigration and Naturalization Serv.*, 533 U.S. 53, 67 (2001) (describing U.S. citizenship as conferring an “absolute right to enter its borders”); U.S. GEN. ACCOUNTING OFFICE, *TRANSPORTATION: EFFORTS TO IMPROVE RECEPTION OF FOREIGN VISITORS AT U.S. AIRPORTS* 5–6 (1991); Jeffrey Kahn, *The Extraordinary Mrs. Shipley: How the United States Controlled International Travel Before the Age of Terrorism*, 43 *CONN. L. REV.* 819 (2011).

39. *United States v. Ramsey*, 431 U.S. 606, 616 (1977); see Kalhan, *supra* note 1, at 1189–97; *Immigration Inspections When Arriving in the U.S.*, TRAC IMMIGRATION (Apr. 4, 2006), <http://trac.syr.edu/immigration/reports/142>. While “non-routine” searches or seizures at the border must be justified by reasonable suspicion, courts have established a high threshold to deem searches or seizures non-routine, and the Supreme Court has applied a lower standard for non-routine border searches and seizures than the probable cause standard that ordinarily applies inside the country. *United States v. Montoya de Hernandez*, 473 U.S. 531, 551 (1985).

40. See Nancy Morawetz, *The Invisible Border: Restrictions on Short-Term Travel by Noncitizens*, 21 *GEO. IMMIGR. L.J.* 201 (2007) [hereinafter Morawetz, *Invisible Border*]; Nancy Morawetz, *Rethinking Drug Inadmissibility*, 50 *WM. & MARY L. REV.* 163 (2008).

processing, and sharing of detailed personal information about all prospective entrants.⁴¹

First, before even seeking to enter the United States, noncitizens are scrutinized more closely than ever before when applying for visas. Although the State Department plays the primary role in processing visa applications, Congress has authorized DHS to assign its own personnel to diplomatic posts to advise and train consular officers, conduct investigations, and review consular decisions. Congress has mandated in-person interviews for most nonimmigrant visa applicants, who are also subject to more intensive background checks.⁴² Moreover, while noncitizens from countries designated under the Visa Waiver Program have been permitted since 1986 to enter the United States without visas as short-term visitors, Congress and DHS more recently have mandated these individuals to apply online for advance “authorization” to enter before commencing their travel.⁴³ Noncitizens admitted to the United States as refugees are also now subject to detailed and lengthy background checks.⁴⁴

Second, both noncitizens and U.S. citizens face increased scrutiny during their travel to the United States. International carriers have long been required to ensure that their passengers are legally authorized to enter the United States and may be held liable for failure to do so.⁴⁵ Beginning in 1988, at the request of U.S. officials, many carriers voluntarily began to transmit personal information collected prior to departure from passengers and other sources to U.S. officials while en route to the United States in order to facilitate efficient customs and immigration screening upon arrival.⁴⁶

41. See NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 416–19 (2004) [hereinafter 9/11 COMM'N REPORT].

42. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004); Homeland Security Act of 2002 § 428, Pub. L. 107-296, 116 Stat. 287 (2002); KEVIN R. JOHNSON, RAQUEL E. ALDANA, BILL ONG HING, LETICIA SAUCEDO, & ENID TRUCIOS-HAYNES, UNDERSTANDING IMMIGRATION LAW 287–95 (2009).

43. 8 U.S.C. § 1187 (2013); Implementing Recommendations of the 9/11 Commission Act of 2007 § 711, Pub. L. 110-53, 121 Stat. 338 (2007); Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. 107-173, 116 Stat. 543 (2002); A. James Vazquez-Azpiri & Daniel C. Horne, *The Doorkeeper of Homeland Security: Proposals for the Visa Waiver Program*, 16 STAN. L. & POL'Y REV. 513, 524–28 (2005).

44. U.N. HIGH COMM'R FOR REFUGEES, THE EFFECTS OF NEW UNITED STATES SECURITY SCREENING MEASURES FOR REFUGEES (2012).

45. Janet A. Gilboy, *Implications of “Third-Party” Involvement in Enforcement: The INS, Illegal Travelers, and International Airlines*, 31 LAW & SOC'Y REV. 505 (1997).

46. EDWARD ALDEN, THE CLOSING OF THE AMERICAN BORDER: TERRORISM, IMMIGRATION, AND SECURITY SINCE 9/11, at 28–32 (2009); U.S. GEN. ACCOUNTING OFFICE, *supra* note 38, at 5–6.

In the wake of the 2001 terrorist attacks, Congress and DHS mandated all commercial airlines and sea carriers to transmit this information to U.S. officials prior to departure, both to facilitate customs and immigration screening and to assess potential risks posed by both noncitizen and U.S. citizen travelers.⁴⁷ In addition, although formal inspection and admission of travelers ordinarily takes place upon arrival at official U.S. ports of entry, individuals traveling from some countries are subject to “preinspection” before they commence their travel by U.S. officials posted extraterritorially at ports of embarkation.⁴⁸ Since 2004, DHS also has posted “advisory personnel” in several countries to help airline employees and airport officials review travel documents and screen travelers for security and public safety risks on U.S.-bound flights, and in some instances to make recommendations that airlines not board particular travelers.⁴⁹

Finally, both citizens and noncitizens are now scrutinized more closely when they arrive and seek to enter the United States. Over 400 million noncitizens and U.S. citizens lawfully enter the United States at official ports of entry each year—with approximately one-quarter of them arriving by air—and border inspectors now conduct more intensive scrutiny to determine their admissibility and any risks they might present.⁵⁰ Congress has conferred inspectors with wide latitude to use a streamlined mechanism, expedited removal, to turn

47. Intelligence Reform and Terrorism Prevention Act of 2004 § 4012, Pub. L. No. 108-458, 118 Stat. 3714 (2004); Enhanced Border Security and Visa Entry Reform Act § 402, Pub. L. No. 107-153, 116 Stat. 543 (2002); Aviation and Transportation Security Act § 115(c), Pub. L. No. 107-71, 115 Stat. 597 (2001); *see infra* Part II.B.3. Noncitizen travelers are inadmissible if they decline to provide this advance passenger information to carriers, and U.S. citizens who decline to provide this information may be prohibited from traveling by the carrier or subjected to greater scrutiny upon arrival in the United States. DEP’T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM (APIS) (2007).

48. 8 U.S.C. § 1225(a) (2013); U.S. CUSTOMS AND BORDER PROTECTION, FACT SHEET: PRECLEARANCE OPERATIONS 1 (May 2013), http://www.cbp.gov/sites/default/files/documents/preclearance_factsheet_2.pdf; Harry Hiller, *Airports as Borderlands: American Preclearance and Transitional Spaces in Canada*, 25 J. BORDERLANDS STUD. 19, 21–27 (2010).

49. While these U.S. officials lack authority to prohibit individuals from traveling to the United States, airlines generally comply with their no-board recommendations, given the risk of being denied landing and the potential sanctions they might face if individuals are refused admission upon arrival. U.S. CUSTOMS AND BORDER PROTECTION, FACT SHEET: IMMIGRATION ADVISORY PROGRAM (IAP) (May 2013), http://www.cbp.gov/sites/default/files/documents/immig_advis_prog_2.pdf; *see also* LISA SEGHELLI, CONG. RESEARCH SERV., BORDER SECURITY: IMMIGRATION INSPECTIONS AT PORT OF ENTRY 10 (2014).

50. MEISSNER ET AL., *supra* note 5, at 57–58.

away noncitizens deemed inadmissible on specified grounds upon their arrival without further adjudication.⁵¹ U.S. officials also have been more assertive in restricting international travel by U.S. citizens, including their entry into the United States—for example, by confiscating or revoking their passports while abroad, prohibiting travel by air or sea, or creating other obstacles to entry.⁵² In addition, both noncitizens and U.S. citizens increasingly have been subject to more intrusive questioning or searches and seizures at the border—for example, the seizure, imaging, and search of computer hard drives and other electronic storage media—with little if any judicial oversight.⁵³

51. 8 U.S.C. § 1225(b)(1)(B)(iii)(I); see Lisa J. LaPlante, *Expedited Removal at U.S. Borders: A World Without a Constitution*, 25 N.Y.U. REV. L. & SOC. CHANGE 213 (1999); Jaya Ramji, *Legislating Away International Law: The Refugee Provisions of the Illegal Immigration Reform and Immigrant Responsibility Act*, 37 STAN. J. INT'L L. 117 (2001).

52. Jeffrey Kahn, *International Travel and the Constitution*, 56 UCLA L. REV. 271 (2008); Leti Volpp, *Citizenship Undone*, 75 FORDHAM L. REV. 2579 (2007); Amel Ahmed, *Yemeni-Americans Cry Foul over Passport Revocations*, AL JAZEERA AM. (Jan. 21, 2014), <http://alj.am/1dN18A5>; Nick Baumann, *Can the Government Confiscate a Citizen's Passport for No Apparent Reason? It Just Did*, MOTHER JONES (Apr. 14, 2014), <http://www.motherjones.com/politics/2014/04/us-passport-confiscated-embassy-nader-el-dajani>; Cyrus Farivar, *Snowden Speaks: By Revoking Passport, US Gov't Is "Using Citizenship as a Weapon"*, ARS TECHNICA (Jul. 1, 2013), <http://ars.to/11bF3G2>; Glenn Greenwald, *US Muslim Placed on No-Fly List Is Unable to See His Ailing Mother*, GUARDIAN (Nov. 5, 2012), <http://gu.com/p/3btaf/tw>; Identity Project, *Does a U.S. Citizen Need the Government's Permission to Return to the U.S.?*, PAPERS, PLEASE (Jan. 28, 2014), <http://papersplease.org/wp/2014/01/28/does-a-us-citizen-need-the-governments-permission-to-return-to-the-us/>; SEGHETTI, *supra* note 48, at 10. The legality of these practices has been sharply questioned. See ASIAN AMERICANS ADVANCING JUSTICE ET AL., STRANDED ABROAD: SHADOW REPORT ON COERCIVE INTERROGATIONS AND DUE PROCESS VIOLATIONS IN THE CONFISCATION OR REVOCATION OF PASSPORTS OF AMERICAN CITIZENS OF YEMENI ORIGIN (2014); Ramzi Kassem, *Passport Revocation As Proxy Denaturalization: Examining the Yemen Cases*, 82 FORDHAM L. REV. 2099 (2014); Patrick Weil, *Citizenship, Passports, and the Legal Identity of Americans: Edward Snowden and Others Have a Case in the Courts*, 123 YALE L.J. F. 565 (2014). For legal challenges, see, for example, *Hizam v. Clinton*, No. 11 Civ. 7693, 2012 WL 3116026, at *2 (S.D.N.Y. July 27, 2012), *rev'd sub nom.* *Hizam v. Kerry*, 747 F.3d 102 (2d Cir. 2014); *Complaint, Nagi v. Kerry*, No. 14 Civ. 13948 (E.D. Mich. Oct. 14, 2014), ECF No. 1, available at <http://klhn.co/Nagi-EDMich-ECF-1>; Kassem, *supra*, at 2107 n.56.

53. RACHEL LEVINSON-WALDMAN, BRENNAN CTR. FOR JUSTICE, WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA 34–38 (2013); Benjamin J. Rankin, *Restoring Privacy at the Border: Extending the Reasonable Suspicion Standard for Laptop Border Searches*, 43 COLUM. HUM. RTS. L. REV. 301 (2011); Ahmed Shihab-Eldin, *Davos to Detention: Why I Hate Coming Home to America*, HUFF. POST (Jan. 28, 2014), <http://huff.to/1aFH5Dq>; Zack Whitaker, *Welcome to the United States: Discriminated, Detained, Searched, Interrogated*, ZDNET (Aug. 31, 2013), <http://zd.net/14gUXez>; compare *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc) (requiring reasonable suspicion, upon an individual's arrival at the border, to copy and conduct a forensic examination of the individual's computer hard drive, but finding that reasonable suspicion was satisfied); with *Abidor v. Napolitano*, 990

While individuals previously could travel between the United States and Mexico, Canada, and the Caribbean without passports, all U.S. citizens and noncitizens are now required to possess a passport or other approved travel document to enter the United States under most circumstances.⁵⁴ DHS also now exercises greater scrutiny over the rapidly growing number of individuals enrolled in its registered traveler programs. These programs provide expedited immigration and customs processing and more limited airport security screening to approved U.S. citizen and noncitizen travelers who submit detailed personal information and, following government background checks, are deemed to present low risks.⁵⁵

B. Direct Post-Entry Monitoring and Enforcement

Among the policy shifts most widely analyzed by immigration law scholars has been the growth of direct, post-entry enforcement within the United States. Historically, once noncitizens had entered the country, immigration officials made little sustained effort to oversee their presence or investigate grounds for their potential deportation. Even when Congress first began to enact post-entry deportability grounds, their scope remained limited. Deportability grounds typically carried statutes of limitations, and opportunities for discretionary relief from deportation were made widely available based on an individualized assessment of factors, including rehabilitation, the effect of deportation on family members, community involvement, and ties to country of origin.⁵⁶

In recent decades, however, the regulation of immigration after noncitizens have entered the United States has increased dramatically. In part, post-entry enforcement serves as an extension of regulation of the territorial border, intended to apprehend noncitizens who are unlawfully present. Under what Daniel Kanstroom terms an “extended border control” model of

F. Supp. 2d 260 (E.D.N.Y. 2013) (suggesting, in dicta, that suspicionless searches of electronic devices at the border might be permissible).

54. Intelligence Reform and Terrorism Prevention Act of 2004 § 7209(b), Pub. L. No. 108-458, 118 Stat. 3823 (2004); U.S. CUSTOMS AND BORDER PROTECTION, WHTI [WESTERN HEMISPHERE TRAVEL INITIATIVE] PROGRAM BACKGROUND (2013), <http://www.getyouhome.gov>.

55. Intelligence Reform and Terrorism Prevention Act of 2004 § 7208(k); Enhanced Border Security and Visa Entry Reform Act of 2002 § 302(b)(1), Pub. L. No. 107-173, 116 Stat. 553 (2002).

56. Morawetz, *supra* note 13, at 1938–39; Mae M. Ngai, *We Need a Deportation Deadline*, WASH. POST (Jun. 14, 2005), <http://www.washingtonpost.com/wp-dyn/content/article/2005/06/13/AR2005061301460.html>.

enforcement, officials seek to deport not only unlawful entrants but also the many individuals—estimated in recent years to comprise between forty and fifty percent of all unauthorized migrants—who lawfully enter as temporary nonimmigrants and then overstay or otherwise violate their terms of admission.⁵⁷ But Congress also has fashioned a second model of deportation by expanding the bases upon which individuals who are *lawfully* present may be “delegalized” and deported for post-entry conduct.⁵⁸ The trend toward this model of what Kanstroom calls “post-entry social control” has been particularly severe for individuals with post-entry criminal convictions.⁵⁹ Until the 1980s, only a limited number of serious crimes rendered noncitizens deportable, and in most instances, those individuals could seek discretionary relief from deportation. Since 1988, however, Congress has steadily (and at times retroactively) expanded the list of criminal deportability grounds to include a broad range of comparatively minor crimes, including a variety of misdemeanors and nonviolent felonies, and has sharply narrowed eligibility for discretionary relief.⁶⁰

The consequences have been transformative, as federal officials now place unprecedented emphasis on direct post-entry enforcement within the United States. Over half of all individuals removed in

57. KANSTROOM, *supra* note 12, at 31–42; see PEW HISPANIC CTR., *MODES OF ENTRY FOR THE UNAUTHORIZED MIGRANT POPULATION* (2006); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-411, *OVERSTAY ENFORCEMENT: ADDITIONAL MECHANISMS FOR COLLECTING, ASSESSING, AND SHARING DATA COULD STRENGTHEN DHS'S EFFORTS BUT WOULD HAVE COSTS* (2011). *But see* BRYAN ROBERTS, EDWARD ALDEN & JOHN WHITLEY, COUNCIL ON FOREIGN RELATIONS, *MANAGING ILLEGAL IMMIGRATION TO THE UNITED STATES: HOW EFFECTIVE IS ENFORCEMENT?* 32–33 (2013) (suggesting that the number of new visa overstays “has dropped sharply in the past decade” and prevailing estimates of overstay population “may be inflated”). In addition, although no reliable estimates exist concerning their numbers, some individuals also may be deemed unlawfully present because they entered the United States using false identity documents or genuine documents that were improperly obtained. See KAMAL SADIQ, *PAPER CITIZENS: HOW ILLEGAL IMMIGRANTS ACQUIRE CITIZENSHIP IN DEVELOPING COUNTRIES* (2009); RUTH ELLEN WASEM, CONG. RESEARCH SERV., *IMMIGRATION FRAUD: POLICIES, INVESTIGATIONS, AND ISSUES* 1–2 (2008).

58. Aarti Shahani, *Legalization and De-Legalization*, GOTHAM GAZETTE (Apr. 2006), <http://www.gothamgazette.com/index.php/civil-rights/3205-legalization-and-de-legalization>; see KANSTROOM, *supra* note 12, at 31–42 (discussing growth in “post-entry social control” as model of enforcement); Adam B. Cox & Eric A. Posner, *The Second-Order Structure of Immigration Law*, 59 STAN. L. REV. 809, 835–40 (2007) (describing shift in immigration enforcement from “ex ante” screening in the form of exclusion to “ex post” screening in the form of deportation).

59. KANSTROOM, *supra* note 12, at 31–42.

60. Morawetz, *supra* note 13, at 1938–43; Stumpf, *supra* note 13, at 382–84; see Nancy Morawetz, *Rethinking Retroactive Deportation Laws and the Due Process Clause*, 73 N.Y.U. L. REV. 97 (1998); Kalhan, *supra* note 1, at 1155–56.

recent years have been deported from inside the United States.⁶¹ Since 1999, deportation of individuals with criminal convictions has been the government's highest stated interior enforcement priority, and the number of individuals removed on criminal grounds has increased accordingly.⁶² Of the 391,000 individuals removed in 2011, almost half had a prior conviction, compared to three percent in 1986.⁶³ Moreover, as the U.S. economy has slumped since 2008 and the number of unauthorized migrants has dropped—and as southwestern border enforcement strategies have increasingly emphasized criminal prosecution rather than immediate expulsion—the number of informal, “voluntary” returns without formal removal orders, which typically occur at or near the territorial border, has plummeted.⁶⁴ As a result of these shifts, lawfully present noncitizens have become immigration enforcement targets to a greater extent than ever before, and the number of formal removals arising from interior enforcement activities now significantly dwarfs the number of informal returns arising from apprehensions at or near the territorial border.⁶⁵

This expansion of direct post-entry enforcement consists of several component mechanisms. First, noncitizens have been subject to more extensive, ongoing monitoring and registration requirements while in the United States. While noncitizens have long been required, as a formal matter, to register and be fingerprinted upon arrival, to carry proof of registration at all times within the United States, and to notify immigration officials promptly of changes of

61. DEP'T OF HOMELAND SEC., OFFICE OF IMMIGR. STATS., *supra* note 8, at 6.

62. MARC R. ROSENBLUM & WILLIAM A. KANDEL, CONG. RESEARCH SERV., INTERIOR IMMIGRATION ENFORCEMENT: PROGRAMS TARGETING CRIMINAL ALIENS 12–13 (2012); DEP'T OF HOMELAND SEC., ENDGAME: DETENTION AND REMOVAL STRATEGIC PLAN, 2003–2012, at 3–4 (2003).

63. DEP'T OF HOMELAND SEC., OFFICE OF IMMIGR. STATS., *supra* note 8, at 112.

64. Richard Marosi, *New Border Foe: Boredom—U.S. Agents Fight to Stay Awake as Illegal Crossings Plummet*, L.A. TIMES, Apr. 21, 2011, at 1; Goodman, *supra* note 8; see ROSENBLUM ET AL., *supra* note 8, at 23 (“[T]oday’s deportation system has been transformed from one that relied overwhelmingly on informal returns to one that mainly emphasizes formal removal.”).

65. One study of government records estimates that at least twenty percent of noncitizens removed because of criminal convictions were lawfully present when charged as deportable and then delegalized in the removal process. In addition, the study noted that in a data set consisting of almost 900,000 individuals deported on criminal grounds, the government could not identify the immigration status of approximately 65,000 noncitizens—fully seven percent of the total. HUMAN RIGHTS WATCH, FORCED APART (BY THE NUMBERS): NON-CITIZENS DEPORTED MOSTLY FOR NONVIOLENT OFFENSES 23–26 (2009).

address, these provisions went largely unenforced for decades.⁶⁶ Even today, these registration requirements largely remain a legal fiction.⁶⁷ Nevertheless, in the aftermath of the 2001 terrorist attacks, the government did step up both its formal and informal efforts to monitor certain categories of noncitizens within the United States.⁶⁸ For example, beginning soon after the attacks, the FBI initiated a program of “voluntary” interviews for thousands of Arab and Muslim men with nonimmigrant visas.⁶⁹ In early 2002, the Justice Department announced plans to aggressively enforce the change of address provision, warning of severe adverse consequences for noncompliance.⁷⁰ Later in 2002, the Attorney General initiated the National Security Entry-Exit Registration System (“NSEERS”), which imposed registration requirements on nonimmigrant men who were at least sixteen years old and current or former nationals of twenty-five countries, all but one predominantly Arab or Muslim.⁷¹ Congress and DHS also tightened oversight of international students and

66. 8 U.S.C. §§ 1301–1306 (2013); see *Etuk v. Slattery*, 936 F.2d 1433, 1436–37 (2d Cir. 1991) (discussing registration requirements for permanent residents); Rashad Hussain, *Preventing the New Internment: A Security-Sensitive Standard for Equal Protection Claims in the Post-9/11 Era*, 13 TEX. J. C.L. & C.R. 117, 126–27 (2007) (discussing underenforcement of registration provisions); Nancy Morawetz & Natasha J. Silber, *Immigration Law and the Myth of Comprehensive Registration*, 48 U.C. DAVIS L. REV. (forthcoming 2014) (manuscript at 6, 48), available at <http://ssrn.com/abstract=2469403> (describing the widespread assumption that a comprehensive federal alien registration system exists in practice as a “dangerous myth” and “insidious misconception”).

67. See Morawetz & Silber, *supra* note 66 (manuscript at 27) (“Most noncitizens in the United States are exempt from registration and carry requirements pursuant to statute, regulation, administrative design, and systemic inefficiencies.”).

68. See Rey Koslowski, *Smart Borders, Virtual Borders or No Borders: Homeland Security Choices for the United States and Canada*, 11 LAW & BUS. REV. AM. 527, 533–34 (2005); Victor C. Romero, *Noncitizen Students and Immigration Policy Post-9/11*, 17 GEO. IMMIGR. L.J. 357 (2002).

69. U.S. GEN. ACCOUNTING OFFICE, *HOMELAND SECURITY: JUSTICE DEPARTMENT’S PROJECT TO INTERVIEW ALIENS AFTER SEPTEMBER 11, 2001* (2003); LAWYERS COMMITTEE FOR HUMAN RIGHTS, *ASSESSING THE NEW NORMAL: LIBERTY AND SECURITY FOR THE POST-SEPTEMBER 11 UNITED STATES* 40–41 (2003).

70. MUZAFFAR A. CHISHTI, DORIS MEISSNER, DEMETRIOS G. PAPADEMETRIOU, JAY PETERZELL, MICHAEL J. WISHNIE & STEPHEN W. YALE-LOEHR, *MIGRATION POL’Y INST., AMERICA’S CHALLENGE: DOMESTIC SECURITY, CIVIL LIBERTIES AND NATIONAL UNITY AFTER SEPTEMBER 11*, at 161 (2003). The announcement prompted a deluge of close to one million change-of-address forms to be filed within the year.

71. RIGHTS WORKING GROUP, *THE NSEERS EFFECT: A DECADE OF RACIAL PROFILING, FEAR, AND SECRECY* 15–16 (2012).

schools where they are enrolled to ensure compliance with the terms of student visas.⁷²

Second, DHS has devoted substantially more resources to post-entry investigations.⁷³ In 2002, DHS launched an initiative targeting “absconders” or “fugitives,” categories that it defines to include (1) individuals with removal orders who have not departed the United States and (2) individuals who have otherwise failed to report to ICE when required.⁷⁴ Between 2003 and 2010, funding for these programs spiraled from \$9 million to over \$230 million, increasing the personnel devoted to these programs by more than 1300%.⁷⁵ The operations conducted under these programs have involved tactics ranging from undercover investigations to high profile, paramilitary-style home and workplace raids and blanket community sweeps in apartment complexes, grocery stores, laundromats, and parks.⁷⁶

Third, federal officials have enlisted hundreds of thousands of state and local law enforcement and corrections officials in immigration policing.⁷⁷ These initiatives, whose particular manifestations have evolved swiftly, seek to identify potentially deportable noncitizens by screening individuals when they are arrested, convicted, and incarcerated to determine their citizenship and immigration status and potential deportability. In addition to these federal initiatives, some states and localities unilaterally have sought to become directly involved in immigration policing. For example, several states and localities—most prominently Arizona, with its controversial and widely-noted Senate Bill 1070—have authorized or required law enforcement to inquire about the immigration status of individuals they encounter and in some instances to convey that

72. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-572, STUDENT AND EXCHANGE VISITOR PROGRAM: DHS NEEDS TO ASSESS RISKS AND STRENGTHEN OVERSIGHT FUNCTIONS (2012); Romero, *supra* note 68.

73. See DEP'T OF HOMELAND SEC., *supra* note 62.

74. MARGOT MENDELSON, SHAYNA STROM, & MICHAEL WISHNIE, MIGRATION POL'Y INST., COLLATERAL DAMAGE: AN EXAMINATION OF ICE'S FUGITIVE OPERATIONS PROGRAM (2009).

75. MEISSNER ET AL., *supra* note 5, at 102.

76. MENDELSON ET AL., *supra* note 74, at 6–11; NEW ORLEANS WORKERS' CENTER FOR RACIAL JUSTICE, THE CRIMINAL ALIEN REMOVAL INITIATIVE IN NEW ORLEANS: THE OBAMA ADMINISTRATION'S BRUTAL NEW FRONTIER IN IMMIGRATION ENFORCEMENT (2013); CARDOZO IMMIGR. JUSTICE CLINIC, CONSTITUTION ON ICE: A REPORT ON IMMIGRATION HOME RAID OPERATIONS (2009); Aldana, *supra* note 14.

77. Kalhan, *supra* note 9; see also Jennifer M. Chacón, *A Diversion of Attention? Immigration Courts and the Adjudication of Fourth and Fifth Amendment Rights*, 59 DUKE L.J. 1563, 1579–98 (2010).

information to federal immigration officials.⁷⁸ While the Supreme Court left open the possibility of as-applied challenges to Section 2 when it reviewed SB 1070, it declined to facially invalidate the provision, and it has previously signaled its willingness to tolerate an active role for state and local police in direct immigration enforcement.⁷⁹

Fourth, federal officials have increasingly deployed removal mechanisms involving little or no formal adjudication. As with expedited removal at the border, officials have utilized a number of streamlined mechanisms to expel deportable noncitizens without full administrative hearings. For example, DHS has increasingly relied upon stipulated removal, by which noncitizens agree to entry of formal removal orders while simultaneously waiving the right to full removal hearings before immigration judges, and reinstatement of removal, a mechanism that permits previous removal orders to be reinstated without further adjudication.⁸⁰ Reinstatements of prior removal orders have steadily increased and totaled more than 149,000 in 2012, representing more than one-third of all removal orders, and stipulated removal orders are now estimated to constitute between ten and thirty percent of all removal orders.⁸¹ Each year, removal orders are also issued in absentia and without further adjudication to thousands of noncitizens who fail to appear for hearings, in many cases due to improper notice.⁸² Expedited removal itself also has been extended from the territorial border to the interior of the United States, under provisions permitting its application to noncitizens if they are apprehended within a zone extending 100 miles from the territorial border and are caught within fourteen days

78. S.B. 1070 § 2, 49th Leg., 2d Sess. (Ariz. 2010); see Gabriel J. Chin, Carissa Byrne Hessick, Toni Massaro, & Marc L. Miller, *A Legal Labyrinth: Issues Raised by Arizona Senate Bill 1070*, 25 GEO. IMMIGR. L.J. 47 (2010); Kevin Johnson, *Immigration and Civil Rights: Is the "New" Birmingham the Same as the "Old" Birmingham?*, 21 WM. & MARY BILL RTS. J. 367 (2012); Kalhan, *supra* note 1, at 1164–65.

79. *Arizona v. United States*, 132 S. Ct. 2492, 2507–11 (2012); *Muehler v. Mena*, 544 U.S. 93, 100–01 (2005); Chacón, *supra* note 15, at 580 (arguing that Arizona “effectively green-lighted systematic state and local participation in immigration enforcement”).

80. Jennifer Lee Koh, *Waiving Due Process (Goodbye): Stipulated Orders of Removal and the Crisis in Immigration Adjudication*, 91 N.C. L. REV. 475 (2013); Family, *supra* note 13; ROSENBLUM ET AL., *supra* note 8, at 24–27.

81. DEP’T OF HOMELAND SEC., OFFICE OF IMMIGR. STATS., *supra* note 8, at 5; Koh, *supra* note 80, at 509–10.

82. U.S. DEP’T OF JUSTICE, EXEC. OFFICE OF IMMIGR. REV., FY 2012 STATISTICAL YEAR BOOK H1–H4 (2013); see Lenni B. Benson, *You Can’t Get There from Here: Managing Judicial Review of Immigration Cases*, 2007 U. CHI. LEGAL F. 405, 417–21 (2007).

of their entry.⁸³ Taken together, these means of removal without adjudication have constituted the overwhelming majority of formal removals in recent years. In 2012, for example, it is estimated that approximately seventy-five percent of all removals were effectuated using these mechanisms, an increase from only three percent in 1995 and 1996.⁸⁴

C. Indirect Post-Entry Monitoring and Enforcement

Especially over the past decade, these direct post-entry enforcement programs have been supplemented by a growing number of *indirect* enforcement initiatives.⁸⁵ These indirect initiatives restrict access to rights, benefits, and services on the basis of immigration or citizenship status, thereby requiring both public and private actors—including social service agencies, educational institutions, hospitals, driver’s license bureaus, employers, landlords, and transportation carriers—to verify immigration and citizenship status to make eligibility determinations. These initiatives enforce immigration law indirectly insofar as they are not always intended primarily to apprehend potentially deportable individuals but nevertheless seek to encourage “self-deportation.”⁸⁶ They also can facilitate direct enforcement by collecting and storing information that later can be used to identify and arrest potentially deportable individuals. Indirect enforcement programs can operate more directly when they require reporting of individuals suspected to be potentially deportable to immigration officials.⁸⁷

Since 1986, the principal means of indirect enforcement under federal law has been the Immigration Reform and Control Act’s (“IRCA”) employer sanctions regime, which prohibits employers from knowingly hiring unauthorized workers and requires them to verify

83. 8 U.S.C. § 1225(b) (2013); A.B.A. COMM’N ON IMMIGRATION, *supra* note 5, at 1-43 to 1-44. Albeit less formally, DHS also induces large numbers of noncitizens to “voluntarily” waive rights to full adjudication. Family, *supra* note 13.

84. ROSENBLUM ET AL., *supra* note 8, at 26–27.

85. Kalhan, *supra* note 1, at 1158–60; *see also* Rodríguez, *supra* note 15, at 592–93; Rick Su, *A Localist Reading of Local Immigration Regulations*, 86 N.C. L. REV. 1619, 1642–49 (2008).

86. MARK KRIKORIAN, CTR. FOR IMMIGR. STUD., *DOWNIZING ILLEGAL IMMIGRATION: A STRATEGY OF ATTRITION THROUGH ENFORCEMENT* 5 (2005); William Safire, *Self-Deportation?*, N.Y. TIMES, Nov. 21, 1994, at A15.

87. Kalhan, *supra* note 1; *see* Linda Bosniak, *The Undocumented Immigrant: Contending Policy Approaches*, in *DEBATING IMMIGRATION* 85, 92 (Carol M. Swain ed., 2007) (noting proponents’ view that “verification and reporting requirements serve as an indispensable enforcement supplement”).

the identity and work eligibility of all new hires.⁸⁸ Enforcement of IRCA's civil and criminal sanctions has been uneven at best, but since 2006, DHS has ramped up its workplace enforcement efforts.⁸⁹ Under the Obama Administration, workplace employment strategies have shifted from high profile workplace raids seeking to directly identify and apprehend potentially deportable noncitizens to more indirect initiatives monitoring employers' compliance with IRCA's requirements.⁹⁰

But indirect initiatives to enforce immigration law have not been limited to employer sanctions. For example, Congress has established mandatory eligibility restrictions for certain public benefits programs on the basis of immigration and citizenship status and has authorized state governments to adopt alienage-based restrictions on access to other benefits programs.⁹¹ Congress has sought to regulate migrants' access to state-issued driver's licenses and other identification documents by mandating minimum standards—and in particular, immigration-status-based eligibility requirements—for them to be accepted as identification for certain federal purposes, such as entering federal buildings or boarding commercial airline flights.⁹² Most recently, in adopting the Patient Protection and Affordable Care Act, Congress explicitly barred unauthorized immigrants from participating in the exchanges and temporary high-risk pools established under the law or receiving the legislation's subsidies and

88. Immigration Reform and Control Act, Pub. L. No. 99-603, 100 Stat. 3359 (1986); Wishnie, *supra* note 6. DHS also has cultivated formal partnerships that encourage employers to directly report information on noncitizens suspected to be deportable. Maya Elbert, *ICE Establishes IMAGE Program*, 20 GEO. IMMIGR. L.J. 717 (2006); Darcy Pottle, *Federal Employer Sanctions as Immigration Federalism*, 16 MICH. J. RACE & L. 99 (2010).

89. BRUNO, *supra* note 8; MEISSNER ET AL., *supra* note 5, at 76-87.

90. See Memorandum from Marcy M. Forman, Director, Office of Investigations, U.S. Immigration and Customs Enforcement, *Worksite Enforcement Strategy* (Apr. 30, 2009); Julia Preston, *U.S. Shifts Strategy on Illicit Work by Immigrants*, N.Y. TIMES, Jul. 3, 2009, at A1. Owing to this shift, DHS has audited over 8000 employers and barred 726 employers from participating in federal contracts during the past four years, compared with approximately 500 audits and one barred employer during the final year of the Bush Administration. The number of final orders assessing monetary penalties increased from eighteen in 2008 to well over 300 in the first three quarters of 2011 alone. MEISSNER ET AL., *supra* note 5, at 83.

91. *E.g.*, 8 U.S.C. §§ 1611-1612, 1621-1622, 1632, 1641 (2013); see Michael J. Wishnie, *Laboratories of Bigotry? Devolution of the Immigration Power, Equal Protection, and Federalism*, 76 N.Y.U. L. REV. 493, 513-14 (2001).

92. REAL ID Act of 2005, Pub. L. No. 109-13, Div. B, 119 Stat. 302, 302-23 (2005); Kalhan, *supra* note 15, at 191-93.

credits for health insurance premiums.⁹³ Within the executive branch, on occasion federal prosecutors have applied the criminal prohibition against transporting noncitizens in knowing or reckless disregard of their unlawful entry or presence to domestic transportation carriers, such as bus lines.⁹⁴

State and local governments also have been active in adopting indirect enforcement initiatives.⁹⁵ For example, some jurisdictions have supplemented IRCA with employer sanctions regimes of their own, for which the Supreme Court has recently held that IRCA itself leaves some room.⁹⁶ Other indirect initiatives go well beyond employer sanctions laws by significantly expanding the circumstances in which eligibility criteria for various services and benefits are based on citizenship or immigration status. These initiatives have dramatically expanded the categories of public and private actors that are placed in the position of collecting, storing, verifying, and disseminating immigration and citizenship status information, together with large quantities of other personal information, on a day-to-day basis.⁹⁷

D. Criminal Prosecution of Migration-Related Offenses

The growing convergence between immigration and criminal law enforcement regimes has prompted huge increases in federal

93. 42 U.S.C. § 18032(f)(3) (2013); ALISON SISKIN & ERIKA K. LUNDER, CONG. RESEARCH SERV., TREATMENT OF NONCITIZENS UNDER THE AFFORDABLE CARE ACT (2014); Polly J. Price, *Can U.S. Immigration Law Be Reconciled with the Protection of Public Health?*, 17 N.Y.U. J. LEGIS. & PUB. POL'Y (forthcoming 2014), available at <http://ssrn.com/abstract=2397524>; Elise Foley, *Affordable Care Act Won't Apply to Immigrants Granted Deferred Action*, HUFF. POST, (Aug. 31, 2012), <http://huff.to/Q7vJuA>; Michael K. Gusmano, *Undocumented Immigrants in the United States: U.S. Health Policy and Access to Care*, UNDOCUMENTED PATIENTS (Oct. 3, 2012), <http://www.undocumentedpatients.org/issuebrief/health-policy-and-access-to-care/>; Esther Yu-Hsi Lee, *A Simple Guide To The Affordable Care Act For Immigrants*, THINKPROGRESS (Oct. 1, 2013), <http://thkpr.gs/1hiY8YU>.

94. Eisha Jain, *Immigration Enforcement and Harboring Doctrine*, 24 GEO. IMMIGR. L.J. 147 (2010); Huyen Pham, *The Private Enforcement of Immigration Laws*, 96 GEO. L.J. 777, 793–96 (2008).

95. *2012 Immigration-Related Laws and Resolutions in the States*, NAT'L CONF. OF STATE LEGISLATURES (2013), <http://www.ncsl.org/issues-research/immig/2012-immigration-related-laws-jan-december-2012.aspx>.

96. *Chamber of Commerce v. Whiting*, 131 S. Ct. 1968 (2011) (holding that Arizona's employer sanctions scheme was not preempted); see *DeCanas v. Bica*, 424 U.S. 351 (1976) (holding that pre-IRCA California employers sanctions law was not preempted); Kati L. Griffith, *Discovering "Immigration" Law: The Constitutionality of Subfederal Immigration Regulation at Work*, 29 YALE L. & POL'Y REV. 389 (2011).

97. Kalhan, *supra* note 1.

criminal prosecutions for immigration enforcement purposes.⁹⁸ Federal prosecutions for migration-related offenses have spiked in recent years, from approximately 7,000 in 1992 to almost 100,000 in 2013.⁹⁹ Much of the recent increase may be attributed to “Operation Streamline,” an initiative in districts along the U.S.-Mexico border in which ICE and CBP officials—who previously referred only the most severe violations for criminal prosecution—routinely refer unlawful border crossers to be prosecuted for illegal entry or reentry, rather than informally or formally removing them.¹⁰⁰ As a result, federal prosecutors now prosecute more migration-related offenses than all other categories of crime combined, of which approximately two-thirds come from southwestern border districts.¹⁰¹ The overwhelming majority of immigration-related criminal convictions have been for illegal entry or reentry. Prosecutions for more serious or complex migration-related offenses, such as human smuggling, human trafficking, migration-related fraud, and willful hiring of unauthorized workers, remain exceedingly less prevalent.¹⁰²

98. Chacón, *supra* note 7; Eagly, *supra* note 7. By one count, federal law includes at least forty-seven separate provisions for immigration-related criminal offenses. Kris W. Kobach, *The Quintessential Force Multiplier: The Inherent Authority of Local Police to Make Immigration Arrests*, 69 ALB. L. REV. 179, 219–21 (2005). Several states have also adopted migration-related criminal offenses. The Supreme Court’s decision in *Arizona v. United States*, which invalidated SB 1070’s criminal provisions as preempted, has trimmed the sails of these efforts. However, it remains to be seen whether *Arizona* leaves room for states and localities to enforce criminal laws touching upon migration-related matters less directly—for example, laws that are formally of general applicability, such as those criminalizing human trafficking and identity theft, but motivated by immigration-related aims or targeting conduct associated with migration. Ingrid V. Eagly, *Local Immigration Prosecution: A Study of Arizona Before SB 1070*, 58 UCLA L. REV. 1749 (2010); Su, *supra* note 85, at 1649–53 (discussing “neutral” local regulations that disproportionately affect noncitizens and are “enacted and enforced precisely for this reason”).

99. *At Nearly 100,000, Immigration Prosecutions Reach All-Time High in FY 2013*, TRAC IMMIGR. (Nov. 25, 2013), <http://trac.syr.edu/immigration/reports/336>.

100. ALISTAIR GRAHAM ROBERTSON, RACHEL BEATY, JANE ATKINSON & BOB LIBAL, GRASSROOTS LEADERSHIP, OPERATION STREAMLINE: COSTS AND CONSEQUENCES (2012); Joanna Lydgate, *Assembly-Line Justice: A Review of Operation Streamline*, 98 CAL. L. REV. 481 (2010); Fernanda Santos, *Detainees Sentenced in Seconds in “Streamline” Justice on Border*, N.Y. TIMES, Feb. 12, 2014, at A12; Donald Kerwin & Kristen McCabe, *Arrested on Entry: Operation Streamline and the Prosecution of Immigration Crimes*, MIGRATION POL’Y INST. (Apr. 29, 2010), <http://www.migrationpolicy.org/article/arrested-entry-operation-streamline-and-prosecution-immigration-crimes>.

101. MEISSNER ET AL., *supra* note 5, at 93–94.

102. *Immigration Prosecutions for April 2014*, TRAC IMMIGR., (Jul. 3, 2014), <http://trac.syr.edu/tracreports/bulletins/immigration/monthlyapr14/fil>.

E. Exit Controls

Finally, DHS has implemented mechanisms to monitor and control departures from the United States. In a series of laws dating back to 1996, Congress has mandated the establishment of a comprehensive, automated system to monitor and collect records of the departure of every noncitizen lawfully admitted to the United States.¹⁰³ This system seeks to match departure records with arrival records to confirm whether noncitizens admitted under temporary, nonimmigrant admission categories have departed the United States when required and to identify individuals who have “overstayed.” As with screening and registration upon initial entry, a complete exit control system necessarily involves monitoring and verifying citizenship and immigration status for all individuals traveling from the United States. Increasingly, exit controls have been justified with reference to national security and criminal law enforcement.¹⁰⁴ At some locations along the U.S.-Mexico border, departing individuals are subject to additional screening under initiatives that target drug trafficking.¹⁰⁵ Other mechanisms restrict the ability of noncitizens to travel outside the United States altogether.¹⁰⁶

While implementation of this system has proven challenging, the federal government has continued to make considerable investments in its development and automation. Under the system in place for many years, nonimmigrants would fill out an I-94 arrival/departure form when seeking admission at the border. Upon admission, border inspectors would stamp and retain this form, returning to individuals a departure receipt to be submitted to transportation carriers upon departure and then forwarded to immigration officials.¹⁰⁷ This process has recently been automated for individuals arriving by air and sea, and immigration officials have piloted automated systems to track exits by verifying and collecting biometric identification

103. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004); Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, 116 Stat. 543 (2002); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 § 414, Pub. L. No. 107-56, 115 Stat. 272 (2001); Immigration and Naturalization Service Data Management Improvement Act of 2000, Pub. L. No. 106-215, 114 Stat. 337 (2000); Illegal Immigration Reform and Immigrant Responsibility Act § 110, Pub. L. No. 104-208, 110 Stat. 3009 (1996).

104. *See, e.g.*, MEISSNER ET AL., *supra* note 5, at 57–59.

105. SEGHETTI, *supra* note 49, at 20–21.

106. Morawetz, *Invisible Border*, *supra* note 40, at 205–20; *see also* MASSEY ET AL., *supra* note 24, at 105–18, 126–36.

107. ALDEN, *supra* note 46, at 66.

information from these travelers.¹⁰⁸ Immigration reform proposals in Congress would go further by requiring air and sea carriers to collect exit data from passengers before departing the United States.¹⁰⁹

II. THE NEW SURVEILLANCE INFRASTRUCTURE OF MASS IMMIGRATION ENFORCEMENT

As these immigration enforcement activities have widely proliferated, and the scale of the enforcement regime's "formidable machinery" has grown and solidified, authorities have deployed a variety of new surveillance, dataveillance, and tracking systems as key components of their enforcement strategies at every stage of the migration process.¹¹⁰ In this Part, I analyze the swift, extensive, and largely unconstrained implementation of these technologies, which have given rise to what I term, adapting from Jack Balkin, the *immigration surveillance state*: an approach to immigration governance "that features the collection, collation, and analysis of information about populations . . . to identify problems, to head off potential threats, to govern populations, and to deliver valuable social services."¹¹¹ These systems enable and routinize the collection, storage, aggregation, processing, and dissemination of detailed personal information for immigration control and other purposes on an unprecedented scale and facilitate the involvement of an escalating number of federal, state, local, private, and non-U.S. actors in immigration control activities.

First, I develop and articulate a framework within which to analyze these developments, disaggregating "immigration enforcement" as a category to identify and analyze the specific purposes for which new surveillance processes and systems have been implemented. These purposes fall into four broad categories:

108. Interim Final Rule, Electronic Form I-94, 78 Fed. Reg. 18457 (Mar. 27, 2013) (codified at 8 C.F.R. § 1.4 (2014)); REY KOSLOWSKI, REAL CHALLENGES FOR VIRTUAL BORDERS: THE IMPLEMENTATION OF US-VISIT 6–7 (2005); Mark Stevens, *Exit Tracking: Should the Federal Government Track Noncitizens' Departures from the United States?*, 3 AM. U. NAT'L SECURITY L. BRIEF 11 (2012).

109. Border Security, Economic Opportunity and Immigration Modernization Act of 2013, S. 744, 113th Cong. § 3303 (as passed by Senate, June 27, 2013); MEISSNER ET AL., *supra* note 5, at 58–59; *see* CTR. FOR IMMIGR. STUD., TEN REASONS WHY BIOMETRIC EXIT MAY ADVANCE IN 2014 (2014).

110. MEISSNER ET AL., *supra* note 5; *see* Edward Alden, *Immigration and Border Control*, 32 CATO J. 107, 114 (2012) ("Entry into the United States from overseas now involves passing through an extraordinary, high-technology security gauntlet . . .").

111. Balkin, *supra* note 4, at 3 (conceptualizing "national surveillance state"); *see* Ho-sein, *supra* note 23; Kalhan, *supra* note 9, at 1109–10.

identifying individuals, screening and authorizing individuals, tracking and controlling mobility, and sharing information. Second, I highlight and assess the deployment of new technologies—across all of the different enforcement initiatives discussed in Part I—to control the territorial border, to monitor and regulate entry, exit, and travel by both noncitizens and U.S. citizens, and to monitor and regulate noncitizens after entry into the United States.

A. *The Functions and Practices of Immigration Surveillance*

As conceptualized by John Gilliom and Torin Monahan, surveillance involves “the systematic monitoring, gathering, and analysis of information in order to make decisions, minimize risk, sort populations, and exercise power.”¹¹² In this Section, I identify and analyze a series of specific surveillance practices and technologies that have become increasingly important components of immigration enforcement strategies. The processes and technologies that comprise the information infrastructure of immigration enforcement enable new approaches to four distinct sets of surveillance activities: *identification, screening and authorization, mobility tracking and control, and information sharing.*

1. *Identification*

Perhaps as much as anything else, the recent expansion of immigration enforcement has helped spark heightened attention to identification—and in particular, the deployment of systems that seek to authenticate or verify the identity of a particular individual (“Is this person who she says she is?”) or to ascertain the identity of an unknown individual (“Who is this person?” or “Who generated this biometric?”).¹¹³ Identification mechanisms, of course, have always been a central element of immigration regulation. While one’s identity ordinarily plays no role in most aspects of day-to-day life for

112. GILLIOM & MONAHAN, *supra* note 4, at 2; see LYON, *supra* note 4, at 14 (defining surveillance as the “focused, systematic, and routine attention to personal details for purposes of influence, management, protection, or direction”); Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498, 499 (1988) (conceptualizing “dataveillance” as “the systematic use of personal data systems in the investigation or monitoring of the actions . . . of one or more persons”); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 490–91 (2005) (advancing “taxonomy” of “privacy problems” that arise from collection, processing, and dissemination of personal information).

113. JENNIFER LYNCH, FROM FINGERPRINTS TO DNA: BIOMETRIC DATA COLLECTION IN U.S. IMMIGRANT COMMUNITIES AND BEYOND 5 (2012); see BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD, 181–206 (2003) (distinguishing among identification, authentication, and authorization in security systems).

either noncitizens or U.S. citizens, rules governing admissibility or deportability necessarily require authorities to accurately identify and determine the particular individuals who are eligible for admission or subject to deportation.¹¹⁴ Debates over the proper role and scope of identification systems for immigration regulation purposes—including most prominently, in recent decades, the potential role of a mandatory, standardized national ID card—have accordingly persisted and recurred over many generations.¹¹⁵

Even as debates over the appropriate role of identification systems in immigration governance have assumed renewed prominence in recent years—as they have, increasingly, in debates about governance more generally—a set of de facto national identification systems already are taking shape.¹¹⁶ Although current efforts to develop identification systems for immigration control purposes have origins in initiatives taken during the 1990s, the aftermath of the 2001 terrorist attacks has hastened their development. In its reports, the September 11 Commission emphasized the ability of the 2001 hijackers to obtain various U.S. identification documents, in some cases by fraud, and the failure of immigration and law enforcement officials who they had previously encountered to identify them and ascertain the threats that they posed. Accordingly, the Commission recommended the establishment of a comprehensive screening system that would collect, store, process, and share detailed personal information, along with the development of more secure identification documents, in

114. Kalhan, *supra* note 1, at 1141–42; see DAVID LYON, IDENTIFYING CITIZENS: ID CARDS AS SURVEILLANCE (2009); SCHNEIER, *supra* note 112.

115. Magdalena Krajewska, *The Politics of National Identification Documents in the United Kingdom and the United States, 1915–2010*, at 257–404 (Aug. 2011) (unpublished Ph.D. dissertation, Brandeis University); see A. MICHAEL FROOMKIN & JONATHAN WEINBERG, *HARD TO BELIEVE: THE HIGH COST OF A BIOMETRIC IDENTITY CARD* (2012); SIMSON GARFINKEL, *DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY* 37–67 (2000); JAMES G. GIMPEL & JAMES R. EDWARDS, JR., *THE CONGRESSIONAL POLITICS OF IMMIGRATION REFORM* 88–89, 162–63 (1999); Daniel J. Steinbock, *National Identity Cards: Fourth and Fifth Amendment Issues*, 56 FLA. L. REV. 697 (2004).

116. A. Michael Froomkin, *The Uneasy Case for National ID Cards*, in *SECURING PRIVACY IN THE INTERNET AGE* 295, 308 (Anupam Chander, Lauren Gelman, & Margaret Jane Radin eds., 2008) (arguing that “enormous growth of the ability to link distributed databases means that we already have, or will soon have, a ‘virtual’ national identification system”); see RICHARD L. HASEN, *THE VOTING WARS: FROM FLORIDA 2000 TO THE NEXT ELECTION MELTDOWN* 41–73 (2012) (discussing voter ID laws); CASSANDRA Q. BUTTS & PETER SWIRE, *CTR. FOR AM. PROGRESS, THE ID DIVIDE* (2008); CARL WATNER & WENDY MCELROY, *NATIONAL IDENTIFICATION SYSTEMS: ESSAYS IN OPPOSITION* (2004); Cristina Costantini, *Municipal ID Cards Given To Undocumented Immigrants In Cities Across The U.S. With Varied Success*, HUFF. POST (Oct. 24, 2011), <http://huff.to/qSpa8q>.

order to identify individuals at the border and in a range of other areas of social life within the United States in order to assess any risks that they might present.¹¹⁷

Infused with this national security significance—and substantial resources, as a result—immigration authorities have implemented a complex and far-reaching set of identification systems.¹¹⁸ Officials now collect large quantities of personal information about both noncitizens and U.S. citizens in a variety of different contexts. In line with the September 11 Commission’s recommendations—but building upon nascent initiatives already under way before the 2001 terrorist attacks—these systems collect not only biographic data but also biometric identifiers, which are “unique markers that identify or verify the identity of people using intrinsic physical or behavioral characteristics,” such as fingerprints, facial recognition-ready digital photographs, iris scans, DNA, palm prints, hand vein scans, or voice prints.¹¹⁹ Based on the supposition that automated biometric processes enable efficient and highly accurate identification of individuals, their use has exploded since 2001, with immigration control serving as a leading edge of this trend.¹²⁰

Immigration authorities store this biographic and biometric information in a growing system of interoperable databases. At the core of this database network is DHS’s Automated Biometric Identification System (“IDENT”), which INS originally developed to help the Border Patrol identify and track individuals unlawfully crossing the U.S.–Mexico border. Today, IDENT is used for a much broader variety of immigration and security-related functions and constitutes the main DHS-wide biographic and biometric information

117. 9/11 COMM’N REPORT, *supra* note 41, at 383–90; see NAT’L COMM’N ON TERRORIST ATTACKS UPON THE UNITED STATES, 9/11 AND TERRORIST TRAVEL: STAFF REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (2004) [hereinafter TERRORIST TRAVEL REPORT].

118. JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 27–28 (2014); Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 425 (2012).

119. LYNCH, *supra* note 113, at 4; see also 9/11 COMM’N REPORT, *supra* note 41, at 383–90; JOSEPH N. PATO & LYNETTE I. MILLETT, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 31–36 (2010).

120. SHOSHANA AMIELLE MAGNET, WHEN BIOMETRICS FAIL: GENDER, RACE, AND THE TECHNOLOGY OF IDENTITY 10 (2011) (“Biometrics are celebrated as perfect identification technologies.”); see NAT’L SCI. & TECH. COUNCIL, BIOMETRICS IN GOVERNMENT POST-9/11: ADVANCING SCIENCE, ENHANCING OPERATIONS (2008) [hereinafter BIOMETRICS IN GOVERNMENT POST-9/11]; Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475 (2013).

system.¹²¹ Growing at a rate of ten million new entries per year, IDENT holds records on over 160 million subjects who have had any contact with DHS, other agencies, and even other governments—including visa applicants at U.S. embassies and consulates, noncitizens traveling to and from the United States, noncitizens applying for immigration benefits (including asylum), unauthorized migrants apprehended at the border or at sea, suspected immigration law violators encountered or arrested within the United States, and even U.S. citizens enrolled in DHS's registered traveler programs or who have adopted children from abroad. Given its data collection and retention practices, IDENT also contains fingerprint records for many naturalized U.S. citizens who were fingerprinted before naturalizing and lawfully present noncitizens.¹²² At the same time, IDENT does not include records of noncitizens who have never had any contact with DHS, such as those who entered the United States without inspection.¹²³

Finally, Congress and immigration authorities have required both noncitizen and U.S. citizen travelers to possess secure identification and travel documents that can be linked to these database records.¹²⁴ Noncitizens entering the United States under the Visa Waiver Program must possess machine-readable passports that incorporate biometric identifiers, and the visas issued to other noncitizen travelers by the State Department are now tamper-resistant, machine-readable documents that include biometric identifiers linked to records in DHS's databases. Other identification, travel, and entry documents issued to noncitizens, such as employment authorization documents and permanent resident cards, have similar enhancements.¹²⁵ U.S. citizen travelers also are subject to

121. System of Records Notice for IDENT, 72 Fed. Reg. 31,080 (June 5, 2007). Within DHS, IDENT is managed by the Office of Biometric Identity Management, which in 2013 replaced a program previously known as US-VISIT.

122. Kalhan, *supra* note 9, at 127–28.

123. Internal government documents indicate that DHS may also be retaining in IDENT the fingerprints of all U.S. citizens whose fingerprints have been shared by the FBI through the Secure Communities program. *Id.*; SEGHELLI, *supra* note 49, at 23.

124. Intelligence Reform and Terrorism Prevention Act of 2004 §§ 7209, 7218, Pub. L. No. 108-458, 118 Stat. 3638 (2004); U.S. DEP'T OF STATE, VISA AND PASSPORT SECURITY STRATEGIC PLAN (2007).

125. Enhanced Border Security and Visa Entry Reform Act of 2002 § 303, Pub. L. No. 107-173, 116 Stat. 543 (2002) (mandating use of biometric identifiers in visas and travel documents issued to noncitizens); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act § 403, Pub. L. No. 107-56, 115 Stat. 272 (2001) (mandating biometric collection and screening for all visa applicants); *see* BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 120, at 44–

enhanced identification and travel document requirements. All U.S. citizens must possess a passport or other approved travel document to enter the United States, and since 2007, all newly issued U.S. passports have been so-called “e-passports.” These machine-readable documents not only include electronically printed digital photographs, but also are embedded with radio frequency identification (“RFID”) chips containing biographic and biometric data about the document holder that can be read wirelessly and linked to government databases.¹²⁶ Congress also has enacted legislation providing that state driver’s licenses and ID cards may be accepted for official purposes by federal agencies only if the state satisfies minimum federal standards for eligibility criteria, application procedures, document contents, and document security.¹²⁷

2. *Analysis, Screening, and Authorization*

Hand-in-hand with these identification systems, policymakers have implemented a variety of authorization mechanisms to facilitate large-scale analysis and screening of migrants and travelers, once they have been identified, in the many settings in which immigration control activities now take place and require screening and authorization based on immigration status, citizenship status, or other criteria.¹²⁸ With the widespread expansion of immigration enforcement activities, as discussed in Part I, these settings are now manifold—ranging from U.S. consulates, airline check-in counters, and ports of entry to local police stations, private workplaces, benefits agencies, universities, health insurers and providers, and beyond.¹²⁹

The specific processes and criteria used in these various settings differ depending on the particular context and immigration control

46; KATHERINE GIGLIOTTI & ANN MORSE, *THE ABCS OF IDs FOR U.S. IMMIGRANTS: A PRIMER FOR STATE LEGISLATORS* (2004).

126. Other travel documents approved for U.S. citizens under some circumstances, such as passport cards, enhanced driver’s licenses, and registered traveler documents, have similar enhancements. MONICA NOGUEIRA & NOEL GREIS, *USES OF RFID TECHNOLOGY IN U.S. IDENTIFICATION DOCUMENTS* (2009); Jonathan Weinberg, *Tracking RFID*, 3 I/S: J.L. & POL’Y INFO. SOC’Y 777, 800–02 (2007).

127. Intelligence Reform and Terrorism Prevention Act of 2004 § 7212(b), Pub. L. No. 108-458, 118 Stat. 3638 (2004); REAL ID Act of 2005 § 202, Pub. L. No. 109-13, Div. B, 119 Stat. 302, 302–23 (2005); see Kalhan, *supra* note 15; see also Serge Egelman & Lorrie Faith Cranor, *The Real ID Act: Fixing Identity Documents with Duct Tape*, 2 I/S: J.L. & POL’Y INFO. SOC’Y 149 (2006).

128. SCHNEIER, *supra* note 113, at 183–84; Froomkin, *supra* note 116, at 297 (“People who control resources . . . want or need to know who you really are in order to allow the interaction or transaction, and they want or need to keep a record of it.”).

129. Bosniak, *supra* note 87, at 90–91.

activities involved. In many instances, screening and authorization can involve seemingly straightforward determinations, such as whether individuals are noncitizens or U.S. citizens or whether noncitizens are clearly inadmissible or deportable. However, determinations of citizenship status, potential inadmissibility or deportability, employment authorization, benefits eligibility, and other screening determinations involved in these various immigration enforcement programs often can be more complex than they appear, requiring collection and synthesis of information from multiple sources, interpretation, clarification, analysis, and the exercise of discretion and judgment.¹³⁰ Moreover, in a growing number of situations, these screening determinations are made using predictive, probabilistic risk assessments that may be automated or semi-automated.¹³¹

Screening and authorization systems perform two categories of interrelated, mutually complementary “sorting” functions.¹³² On the one hand, authorities rely upon information in these systems to identify individuals who should be denied authorization in a particular context or who are deemed to require closer attention and scrutiny. For example, actors involved in visa processing, border inspection, and immigration policing screen the names of individuals

130. *Padilla v. Kentucky*, 559 U.S. 356, 377–78 (2010) (Alito, J., concurring) (noting that “whether a conviction for a particular offense will make an alien removable is often quite complex,” and that criminal lawyers “who consult[] a guidebook” to make that determination “will often find that the answer is not ‘easily ascertained’”); Seth M.M. Stodder, *Finding Terrorist Needles: The Automated Targeting System*, 9 ENGAGE: J. FEDERALIST SOC’Y PRAC. GROUPS 84, 85 (2008) (emphasizing complexity of role played by CBP inspectors at ports of entry); see also Kalhan, *supra* note 9, at 1138; Jennifer Lee Koh, *Rethinking Removability*, 65 FLA. L. REV. 1803 (2013); Rachel E. Rosenbloom, *The Citizenship Line: Rethinking Immigration Exceptionalism*, 54 B.C. L. REV. 1965, 1967–68 (2013); Juliet P. Stumpf, *Getting to Work: Why Nobody Cares About E-Verify (And Why They Should)*, 2 U.C. IRVINE L. REV. 381, 392–95 (2012).

131. Stodder, *supra* note 130 (discussing CBP’s Automated Targeting System); WESTAT CORP., *EVALUATION OF THE ACCURACY OF E-VERIFY FINDINGS* 3 (2012) (discussing “complex matching algorithms” and search processes used by E-Verify); see Danielle Keats Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014) (highlighting expanded use of “scoring systems” that aggregate information and use predictive algorithms to score and rank individuals when making various decisions about those individuals); Citron, *supra* note 19, at 1263–67 (identifying and categorizing different types of automated and semi-automated decision-making systems being used in administrative agencies’ decision making processes).

132. David Lyon, *Surveillance as Social Sorting: Computer Codes and Mobile Bodies*, in *SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK, AND DIGITAL DISCRIMINATION* 13, 20 (David Lyon ed., 2003) (discussing use of surveillance “to classify people and populations according to varying criteria, to determine who should be targeted for special treatment, suspicion, eligibility, inclusion, access”).

whom they encounter against information in the FBI's main criminal records database, the National Crime Information Center ("NCIC")—a clearinghouse that includes information on criminal history and outstanding warrants—to determine whether they may be inadmissible to enter the United States or potentially deportable.¹³³ These officials also screen the names of these individuals against watchlists generated from the FBI's Terrorist Screening Database ("TSDB"), a consolidated antiterrorism watchlist containing over one million records on approximately 400,000 subjects identified and designated as known or suspected terrorists. Individuals are periodically added and removed from the TSDB, and from this master database the FBI generates and distributes several more specific lists, such as the No Fly List and the Automatic Selectee List, to various immigration control, criminal law enforcement, and transportation security authorities in the United States and other countries.¹³⁴ Increasingly, employers subject to employer sanctions screen the names of their employees against the federal government's E-Verify database system to determine whether they are authorized to work in the United States.¹³⁵ The Affordable Care Act requires electronic verification of citizenship and lawful presence for all individuals seeking to purchase health insurance through the government-established exchanges, to obtain credits or subsidies for health insurance premiums, or to secure benefits under Medicaid or the Children's Health Insurance Program ("CHIP").¹³⁶

Other systems aggregate and analyze information from a multiplicity of sources to furnish automated, probabilistic risk

133. Kalhan, *supra* note 9 (discussing NCIC).

134. Homeland Security Presidential Directive No. 6, Integration and Use of Screening Information to Protect Against Terrorism (Sep. 16, 2003); WILLIAM J. KROUSE & BART ELIAS, CONG. RESEARCH SERV., TERRORIST WATCHLIST CHECKS AND AIR PASSENGER PRESCREENING (2009); DEP'T OF HOMELAND SEC., OFFICE OF INSPECTOR GEN., ROLE OF THE NO FLY AND SELECTEE LISTS IN SECURING COMMERCIAL AVIATION (REDACTED) 9–16 (2009); U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., FOLLOW-UP AUDIT OF THE TERRORIST SCREENING CENTER 3–6 (2007); Jennifer C. Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327, 344–48 (2014); Peter Shane, *The Bureaucratic Due Process of Government Watch Lists*, 75 GEO. WASH. L. REV. 804, 811–19 (2007). While the government had long resisted disclosing its criteria for adding individuals to the TSDB, an intelligence community source disclosed those guidelines to journalists in 2014. Jeremy Scahill & Ryan Devereaux, *Blacklisted: The Secret Government Rulebook For Labeling You a Terrorist*, INTERCEPT (July 23, 2014), <http://interc.pt/1r8CooO>.

135. Stumpf, *supra* note 130.

136. 42 U.S.C. § 18081 (2013); see CTR. FOR DEMOCRACY & TECH., PRIVACY AND SECURITY IN THE AFFORDABLE CARE ACT'S DATA HUB (2013); SISKIN & LUNDER, *supra* note 93, at 10–13; *Immigrants and the Affordable Care Act (ACA)*, NAT'L IMMIGR. LAW CTR. (2014), <http://www.nilc.org/immigrantshcr.html>.

assessments to officials in real time, with the goal of identifying unknown individuals whose names might not be listed in immigration, criminal records, or antiterrorism databases, but whose information matches previously identified profiles and who therefore are deemed to warrant closer scrutiny. For example, CBP's Automated Targeting System ("ATS"), a "decision support tool" originally developed by the U.S. Customs Service to screen cargo for illegal drugs and other contraband, aggregates detailed information about all travelers entering and leaving the United States and assesses the risks presented by each of them in order to identify and prioritize individuals deemed to warrant greater attention by CBP border inspectors.¹³⁷ The ATS analyzes information collected from a wide variety of different sources, including information collected from transportation carriers about travelers and information contained in a broad array of other government databases.¹³⁸ For domestic flights, the Computer-Assisted Passenger Prescreening System ("CAPPS") operated by the Transportation Security Administration ("TSA") performs a similar role.¹³⁹

On the other hand, these systems (and others) simultaneously are intended to perform a second sorting function by facilitating more rapid, efficient screening and authorization of individuals who are regarded as presenting comparatively low risks. This second dimension of screening and authorization seeks to minimize inconvenience to these individuals but also to permit officials to devote greater attention and resources to those deemed to present higher risks or more complicated situations.¹⁴⁰ With massive numbers of people and volumes of goods entering the United States, and DHS targeting large numbers of noncitizens for investigation and enforcement within the country, officials regard ensuring efficient movement by those believed to present low risks as an imperative—in order, for example, to prevent cross-border traffic from grinding to a halt, as it did in the days immediately following the 2001 terrorist

137. System of Records Notice, Automated Targeting System, 77 Fed. Reg. 30,297, 30,298 (May 22, 2012); KROUSE & ELIAS, *supra* note 134, at 8–11.

138. System of Records Notice, Automated Targeting System, 77 Fed. Reg. at 30,298; KROUSE & ELIAS, *supra* note 134, at 8–11; Ellen Nakashima, *Collecting of Details on Travelers Documented U.S. Effort More Extensive Than Previously Known*, WASH. POST, Sep. 22, 2007, at A1.

139. KROUSE & ELIAS, *supra* note 134, at 13–15.

140. Stodder, *supra* note 130, at 86 (describing ATS as enabling CBP to "identify[] individuals warranting further scrutiny, without creating crippling bottlenecks at the airport" for everyone else); *see* SCHNEIER, *supra* note 113, at 181 (noting that, necessarily, "all security systems need to allow people in, even as they keep people out").

attacks.¹⁴¹ Similar kinds of efficiency and risk management concerns arise in post-entry enforcement programs.

Accordingly, immigration-related screening and authorization mechanisms increasingly have been designed with these efficiency- and risk management-related objectives in mind. For example, DHS has actively encouraged participation in several registered traveler programs—Global Entry, NEXUS, SENTRI, FAST, and TSA PreCheck—under which it collects, maintains, and analyzes detailed information on individuals who have been prescreened and approved as presenting low risks. Applicants to these programs must pay an application fee and submit photographs, fingerprints, and detailed personal information—including current and prior employment information, current and prior residential addresses, travel history, criminal history, and immigration history—and must successfully pass an extensive background check, which includes an in-person interview and a review of criminal history, customs, immigration, agriculture, and national security databases. Whether or not applicants are approved, this information is stored in CBP databases and biometric records are created for all applicants in IDENT. Once approved, these individuals are deemed to require more limited scrutiny when entering the United States and are eligible to enroll in TSA's PreCheck program, a registered traveler program for air travelers believed to present limited risks to aviation security.¹⁴²

Similarly, at certain ports of entry, CBP has deployed automated passport control systems that collect, analyze, and store biographic information, photographs, and travel information from arriving individuals (currently, only U.S. and Canadian citizens and individuals seeking to enter the United States under the Visa Waiver Program) using self-service kiosks—or, in a new pilot program, using smartphone applications—rather than having CBP inspectors manually collect and process that information using paper forms. Individuals must then present their passport and a document generated by the automated system for review by CBP inspectors before they may be authorized to enter the United States. As with its registered traveler programs, these new automated systems are intended not only to facilitate more efficient entry of individuals

141. ALDEN, *supra* note 46, at 42–48; Stephen E. Flynn, *Beyond Border Control*, 79 FOREIGN AFF. 58, 59–62 (2000).

142. *Trusted Traveler Programs*, DEP'T OF HOMELAND SEC., <http://www.dhs.gov/trusted-traveler-programs>; *see also* REY KOSLOWSKI, MIGRATION POL'Y INST., THE EVOLUTION OF BORDER CONTROLS AS A MECHANISM TO PREVENT ILLEGAL IMMIGRATION, 13–14 (2011).

deemed to present low risks after their information has been analyzed and processed, but also to permit officials to identify and sort individuals deemed to present higher risks, so that officials may devote greater attention and scrutiny to those individuals.¹⁴³

3. *Mobility Tracking and Control*

The proliferation of settings in which immigration enforcement activities take place also has given rise to extensive government monitoring and control over travel and mobility of both noncitizens and U.S. citizens. In the wake of the 2001 attacks, travel itself has been deemed a source of potential danger to public safety: in the words of the September 11 Commission, “Targeting travel is at least as powerful a weapon against terrorists as targeting their money.”¹⁴⁴ Accordingly, the Commission recommended that border screening systems be integrated into a broader network of screening systems covering transportation and other sensitive facilities.¹⁴⁵ Government authorities have invested heavily to develop and upgrade systems that collect, analyze, store, and disseminate detailed information about individuals’ mobility and travel plans—both internationally and domestically, and including both noncitizens and U.S. citizens.¹⁴⁶ These travel and mobility tracking systems have been developed within a broader context in which the government’s capacity to undertake day-to-day location tracking, using GPS systems, cellular telephone location data, automated license plate readers, and other mechanisms, has also been significantly enhanced.¹⁴⁷ In combination

143. *Automated Passport Control (APC)*, U.S. CUSTOMS AND BORDER PROTECTION, <http://www.cbp.gov/travel/us-citizens/automated-passport-control-apc>; see Gillian Brockwell, *CBP Brings Automated Services to More Than Just Travel Elite*, FED. NEWS RADIO (Feb. 5, 2013), <http://www.federalnewsradio.com/475/3218839/CBP-brings-automated-services-to-more-than-just-travel-elite>; Ben Mutzabaugh, *Filling Out Your Customs Forms? There’s an App for That . . .*, USA TODAY (Aug. 12, 2014), <http://usat.ly/1orOXxV>.

144. 9/11 COMM’N REPORT, *supra* note 41, at 385; TERRORIST TRAVEL REPORT, *supra* note 117; see ELEC. PRIVACY INFO. CTR., *PRIVACY AND HUMAN RIGHTS 2006: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (2007)* (“Travelers and workers at transportation facilities such as airports have come to be regarded as objects of suspicion, potential terrorists, and targets of surveillance.”).

145. 9/11 COMM’N REPORT, *supra* note 41, at 387.

146. U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-14-62, *BORDER SECURITY: DHS’S EFFORTS TO MODERNIZE KEY ENFORCEMENT SYSTEMS COULD BE STRENGTHENED* (2013); see John Schwartz & Micheline Maynard, *Airlines Gave F.B.I. Millions of Records on Travelers After 9/11*, N.Y. TIMES, May 1, 2004, at A1.

147. *United States v. Jones*, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011); Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could*

with authorization mechanisms that restrict travel for certain individuals, these systems have enabled a comprehensive regime that accumulates and stores detailed, permanent records about individual travel histories and patterns, and enables much individual travel, both international and domestic, only to take place upon receipt of affirmative, advance government permission.¹⁴⁸

Several information systems enable this regime of mass surveillance and control of travel and mobility. As discussed below, CBP collects several categories of personal and travel information from transportation carriers, computerized reservation systems, other government agencies, and directly from individual travelers using a variety of mechanisms—beginning before individuals commence their travel and extending through completion of the inspection process at the port of entry. This information is stored within a series of database systems—but even when it does not store information in its own systems on travel and mobility, DHS has required transportation carriers to provide real time access to obtain this information directly from their reservation and departure control systems.¹⁴⁹ In addition, the new e-passports have the technical capacity to include an archive of the holder’s travel history, although to date this feature has not been activated for U.S. passports.

For both noncitizens and U.S. citizens, individuals’ personal and travel information is stored within ATS and within TECS, a CBP-managed system that officials describe as “one of the largest, most important law enforcement systems currently in use,” a “multifaceted computing platform” that has evolved into a “system of systems.”¹⁵⁰ The system includes multiple databases that aggregate and store many different categories of personal information, including:

Enact, 27 BERKELEY TECH. L.J. 117 (2012); Ellen Nakashima & Josh Hicks, *DHS Seeks System to Track Cars’ License Tags*, WASH. POST, Feb. 19, 2014, at A1.

148. Edward Hasbrouck, *Government Surveillance and Control of Travelers*, Presentation at Cato Institute, Apr. 2, 2013, available at <http://hasbrouck.org/blog/archives/002058.html>.

149. Interim Rule, Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States, 67 Fed. Reg. 42710, 42712 (June 25, 2002) (codified at 19 C.F.R. § 122.49d(c)(ii) (2014)) (requiring carriers to provide CBP “with the necessary airline reservation/departure control systems’ commands” to enable CBP to “[c]onnect to the carrier’s reservation/departure control systems”); see PRIVACY INTERNATIONAL, TRANSFERRING PRIVACY: THE TRANSFER OF PASSENGER RECORDS AND THE ABDICATION OF PRIVACY PROTECTION 2 (2004); Hasbrouck, *supra* note 148.

150. U.S. GOV’T ACCOUNTABILITY OFFICE, *supra* note 146, at 3–4. No longer an acronym, TECS is the successor to the Treasury Enforcement Communications System, which was operated by the U.S. Customs Service before its functions were transferred the Treasury Department to DHS in 2003. *Id.* at 1.

- Passenger and crew information collected and transmitted by transportation carriers;
- Border crossing information on close to one billion travelers who have entered and departed the United States;
- Records on enrolled participants in DHS's registered traveler programs;
- State Department records on U.S. citizens who have been issued passports and other travel documents and on noncitizen visa applicants (including individuals who have been both issued and denied visas);
- USCIS records on over fifty-seven million applicants and petitioners for immigration benefits, including both noncitizens and U.S. citizens; and
- Information from other government databases, such as those maintained by state motor vehicle departments, that facilitate CBP's identification and admissibility determinations for noncitizens and U.S. citizens seeking to enter the United States.

CBP officials use TECS when determining whether noncitizens and U.S. citizens seeking to enter the United States may be admitted. The system enables travelers' information to be compared against antiterrorism watchlists generated by the TSDB, criminal history records in the NCIC, risk assessments generated by the ATS, and immigration history records within TECS itself.¹⁵¹

When individuals enter the United States, records of those border crossings—including narrative reports containing information that CBP inspectors deem relevant to their encounters with travelers—are created and maintained in TECS's Border Crossing Information System ("BCIS"). In addition, for noncitizens, this travel information also is copied and stored in TECS's Arrival and Departure Information System ("ADIS"), which holds detailed biographic and travel records on over 280 million noncitizens who have applied for entry, entered, or departed the United States and

151. System of Records Notice, Border Crossing Information System, 73 Fed. Reg. 43457 (July 25, 2008); DEP'T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING (2010); DEP'T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR CBP PROCEDURES FOR PROCESSING TRAVEL DOCUMENTS AT THE BORDER (2008); U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 146, at 46–47; *see* ANGWIN, *supra* note 118, at 92–95; Hasbrouck, *supra* note 148.

that are linked to the biometric records in IDENT.¹⁵² The primary purpose of ADIS is to monitor and identify temporary nonimmigrants who may have remained in the United States beyond their periods of authorized stay by matching records of arrival and departure.¹⁵³ However, the system also is accessed for other immigration control, law enforcement, and national security purposes. In addition to information collected from individual travelers and transportation carriers, ADIS also holds information collected from colleges and universities on noncitizens admitted on student visas.¹⁵⁴

4. *Information Sharing and Interoperability*

Finally, especially in the aftermath of the 2001 terrorist attacks, information sharing and interoperability of database systems have become high government priorities—particularly for national security purposes, but increasingly for other purposes as well.¹⁵⁵ Accordingly, both Congress and the executive branch have directed the development of a variety of systems and processes to disseminate and share information that might be relevant for security-related purposes among various actors, including intelligence agencies, law enforcement, immigration authorities, international entities, foreign governments, and other institutions, both public and private.¹⁵⁶ In

152. SEGHELLI, *supra* note 49, at 23.

153. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-683, OVERSTAY ENFORCEMENT: ADDITIONAL ACTIONS NEEDED TO ASSESS DHS'S DATA AND IMPROVE PLANNING FOR A BIOMETRIC AIR EXIT PROGRAM, 12-15 (2013).

154. DEP'T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM (ADIS) (2007); SEGHELLI, *supra* note 49, at 23; Systems of Records Notice for Arrival and Departure Information System, 78 Fed. Reg. 31955 (May 28, 2013).

155. 9/11 COMM'N REPORT, *supra* note 41, at 416-19 (urging information sharing "across new networks that transcend individual agencies" for national security purposes); *see also* MARKLE FOUND'N ON NAT'L SEC., MOBILIZING INFORMATION TO PREVENT TERRORISM (2006); Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1448 (2011); Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951 (2006).

156. Implementing Recommendations of the 9/11 Commission Act of 2007 §§ 501-513, 701, 711, 801-804, 1203, 1305, 1410, Pub. No. L. 110-53, 121 Stat. 338 (2007); Intelligence Reform and Terrorism Prevention Act of 2004 §§ 1016, 1021-1023, 1061, 6501, 7204, 7210, Pub. L. No. 108-458, 118 Stat. 3638 (2004); Homeland Security Act of 2002 § 428, Pub. L. 107-296, 116 Stat. 2188-2191 (2002); Enhanced Border Security and Visa Entry Reform Act of 2002 §§ 201-204, 603, Pub. L. 107-173, 116 Stat. 543 (2002); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 § 414, Pub. L. No. 107-56, 115 Stat. 272 (2001); Homeland Security Presidential Directive No. 24, Biometrics for Identification and Screening, ¶ 11 (June 5, 2008).

some instances, these efforts have involved the creation of new institutional forms altogether, such as the “fusion centers” authorized by Congress to “co-locate” federal, state, and local officials together to work collaboratively, along with private contractors, on the collection and analysis of intelligence concerning a broad array of potential threats.¹⁵⁷ In many other instances, they have involved efforts to make government databases interoperable and more widely accessible across agency lines.

This emphasis on interoperability in immigration governance has been particularly great as the federal institutions involved in immigration regulation have become more fragmented. With the creation of the Department of Homeland Security, most immigration policy functions were transferred from a single agency within the Department of Justice (the INS) to multiple agencies within DHS (USCIS, CBP, and ICE)—even as other immigration-related functions have remained vested within the Department of Justice, Department of State, Department of Health and Human Services, and Department of Labor. Moreover, as immigration control activities have proliferated in a variety of new state, local, and private institutions, and the overall scale of enforcement has skyrocketed, the number of public and private actors performing immigration enforcement functions has grown exponentially. In this context, the post-2001 emphasis on information sharing for national security purposes has also given a boost to initiatives to make the technological systems used for immigration control by different agencies interoperable with each other and more widely accessible to different actors involved in immigration enforcement.¹⁵⁸

In this context, these interoperability initiatives have not simply fashioned the “connective tissue” that ties different federal immigration agencies together with each other.¹⁵⁹ They also integrate those institutions with the administrative infrastructure of criminal justice, national security and military defense, employment, transportation, and other federal, state, local, and private institutions—thereby enabling immigration control and enforcement institutions to be used for a range of other purposes. For example,

157. Citron & Pasquale, *supra* note 155, at 1449–55; Torin Monahan & Priscilla M. Regan, *Zones of Opacity: Data Fusion in Post-9/11 Security Organizations*, 27 CAN. J.L. & SOC. 301 (2012).

158. Kalhan, *supra* note 9, at 1126–27 & n.95 (discussing pre-2001 immigration policing initiatives); *see also* MEISSNER ET AL., *supra* note 5, at 77–79 (discussing automated employment eligibility verification pilot programs in the 1990s).

159. MEISSNER ET AL., *supra* note 5, at 65.

IDENT is now interoperable with the FBI's Integrated Automated Fingerprint Identification System ("IAFIS"), which integrates and stores fingerprints and other personal information collected and submitted by federal, state, and local law enforcement agencies and other contributors for over 100 million subjects and links those fingerprint records to criminal history records in databases across the country.¹⁶⁰ Eventually, both of these systems will be made fully interoperable with the Department of Defense's multimodal biometrics database system, Automated Biometric Identification System ("ABIS")—thereby completing the development of what the Defense Department refers to as the "biometrics triad."¹⁶¹ Increasingly, immigration control systems also have become integrated with private information systems, most notably the computerized reservation systems and departure control systems of transportation carriers.

B. Immigration Enforcement as Immigration Surveillance

These four sets of migration and mobility surveillance functions—identification, screening and authorization, mobility tracking and control, and information sharing—play crucial but underappreciated roles in immigration control processes across the entire spectrum of migration and travel. In the growing number of contexts in which immigration control activities now take place, enforcement actors engage in extensive collection, storage, analysis, and dissemination of personal information, in order to identify individuals, screen them and authorize their activities, enable monitoring and control over their travel, and share information with other actors who bear immigration control responsibilities. Initially deployed for traditional immigration enforcement purposes, and expanded largely in the name of security, these surveillance technologies and processes are qualitatively remaking the nature of immigration governance, as a number of examples illustrate.

160. DEP'T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT) 11–15 (2012); *Integrated Automated Fingerprint Identification System*, FED. BUREAU INVEST., http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis.

161. U.S. DEP'T OF DEFENSE, BIOMETRICS IDENTITY MANAGEMENT AGENCY, ANNUAL REPORT FISCAL YEAR 2011, at 18–21 (2012); see U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-276, DEFENSE BIOMETRICS: DOD CAN BETTER CONFORM TO STANDARDS AND SHARE BIOMETRIC INFORMATION WITH FEDERAL AGENCIES 18–26 (2011); see also BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 120, at 24–27; Donohue, *supra* note 118, at 457–59.

1. *Border Control*

Despite implementation challenges, Congress and DHS have placed new surveillance technologies at the heart of border control strategies.¹⁶² Physical barriers along the U.S.-Mexico border have been supplemented with advanced lighting, motion sensors, remote cameras, and mobile surveillance systems, and DHS has deployed a fleet of unmanned aerial vehicles to monitor coastal areas and land borders.¹⁶³ To date, these drones primarily have been used to locate illegal border crossers and individuals suspected of drug trafficking in remote areas using ultra high-resolution cameras, thermal detection sensors, and other surveillance technologies.¹⁶⁴ However, drones also have been used to patrol and monitor activities within Mexico itself.¹⁶⁵ In addition, government documents indicate that DHS's drones are capable of intercepting wireless communications and may eventually incorporate facial recognition technology linked to the agency's identification databases.¹⁶⁶ According to one official, CBP's drones can "scan large swaths of land from 20,000 feet up in the air while still being able to zoom in so close that footprints can be seen on the ground."¹⁶⁷ The DHS has plans both to expand its fleet of drones and to increase their surveillance capabilities, and immigration reform proposals in Congress would significantly build upon these recent expansions.¹⁶⁸

162. CHAD C. HADDAL, YULE KIM & MICHAEL GARCIA, CONG. RESEARCH SERV., BORDER SECURITY: BARRIERS ALONG THE U.S. INTERNATIONAL BORDER (2009).

163. Rey Koslowski, *Immigration Reforms and Border Security Technologies*, BORDER BATTLES (July 31, 2006), <http://borderbattles.ssrc.org/Koslowski>; Greg Beato, *Big Brother's Border Blindness*, REASON, Dec. 2012, at 16; ANDREAS, *supra* note 24, at 91–92; ROSENBLUM, *supra* note 30, at 16–19.

164. CHAD C. HADDAL & JEREMIAH GERTLER, CONG. RESEARCH SERV., HOMELAND SECURITY: UNMANNED AERIAL VEHICLES AND BORDER SURVEILLANCE (2010); DEP'T OF HOMELAND SEC., OFFICE OF INSPECTOR GEN., CBP'S USE OF UNMANNED AIRCRAFT SYSTEMS IN THE NATION'S BORDER SECURITY (2012).

165. Ginger Thompson & Mark Mazzetti, *U.S. Drones Fly Deep in Mexico to Fight Drugs*, N.Y. TIMES, Mar. 16 2011, at A1.

166. Declan McCullagh, *DHS Built Domestic Surveillance Tech into Predator Drones*, CNET (Mar. 2, 2013), <http://cnet.co/ZaD4fa>; ACLU, PROTECTING PRIVACY FROM AERIAL SURVEILLANCE: RECOMMENDATIONS FOR GOVERNMENT USE OF DRONE AIRCRAFT (2011).

167. Hernán Rozemberg, *Homeland Security Expands Use of Drones on the Border*, FRONTERAS (Jul. 3, 2012), <http://www.fronterasdesk.org/content/homeland-security-expands-use-drones-border>.

168. M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, 30 (2011); Jill Replogle, *In Border Security Quest, A Call for More Drones*, FRONTERAS (Feb. 11, 2013), <http://www.fronterasdesk.org/content/border-security-quest-call-more-drones>.

2. *Overseas Visa Issuance and Refugee Processing*

In 2001, Congress mandated the State Department to conduct biometric screening for all visa applications, and by 2004, diplomatic posts worldwide were collecting fingerprints from all visa applicants along with photographs, biographic information, background information, and other personal details.¹⁶⁹ The State Department maintains records on all visa applications, including both issuances and denials, in its Consular Consolidated Database (“CCD”), which holds biometric and biographic records on over 100 million visa cases and grows at a rate of approximately 35,000 visa cases per day.¹⁷⁰ The CCD also holds records on all applicants for U.S. passports and other U.S. citizen services. Through CCD, consular officials run name checks on applicants against the Consular Lookout and Support System (“CLASS”)—a State Department database containing over twenty-six million records collected from individual applicants and the databases of numerous other government agencies—in order to identify individuals who may be ineligible for visa issuance or warrant special handling.¹⁷¹ Now, CCD is also interoperable with DHS’s IDENT and the FBI’s IAFIS systems, which enables consular officials to share visa information and run biometric checks against records in those databases, and with ATS.¹⁷² At some diplomatic posts, consular officials have access to ADIS, which enables them to determine whether applicants have previously “overstayed” while in the United States. Additional screening is conducted by DHS agents assigned to certain diplomatic posts, who have access to TECS and other databases and who conduct more in-depth analysis and investigation of applicants as necessary. With the deployment of new technologies that permit remote review of visa applications by personnel in the United States, this additional layer of DHS review is being extended to all visa applications worldwide.¹⁷³

169. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 § 403(c), Pub. L. No. 107-56, 115 Stat. 272 (2001); BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 119, at 44–46; U.S. DEP’T OF STATE, PRIVACY COORDINATOR, CONSULAR CONSOLIDATED DATABASE (CCD): PRIVACY IMPACT ASSESSMENT (2010).

170. U.S. DEP’T OF STATE, *supra* note 169.

171. *Id.*

172. BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 120, at 44–46; U.S. DEP’T OF STATE, *supra* note 169.

173. RUTH ELLEN WASEM, CONG. RESEARCH SERV., VISA SECURITY POLICY: ROLES OF THE DEPARTMENTS OF STATE AND HOMELAND SECURITY 7 (2011); DEP’T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE VISA SECURITY PROGRAM TRACKING SYSTEM—NETWORK VERSION 2.0 (2013).

Overseas processing of refugees also now involves an intensive process of information collection, screening, and dissemination, including biographic and biometric background checks against the databases of multiple government agencies.¹⁷⁴ In a recent pilot program, the State Department collected and tested DNA from African refugees seeking to reunite with relatives in the United States in order to detect fraudulent family reunification claims. As a result of that pilot program, the State Department suspended its refugee family reunification program in certain parts of Africa, and when it resumed that program in 2012, the State Department instituted rules that made DNA testing mandatory to establish the legitimacy of certain claimed family relationships.¹⁷⁵

3. *Entry, Exit, and Travel Control*

CBP and TSA collect, analyze, store, and disseminate large quantities of detailed personal information and travel history about both noncitizens and U.S. citizens arriving in or departing from the United States by air or sea before they commence their travel. More recently, this same basic system has been extended to domestic travel by air within the United States, thereby integrating the surveillance and tracking mechanisms for both domestic and international travel. As a result of these systems, much travel now only can take place after carriers receive affirmative, advance government permission to permit individuals to travel—without travelers themselves necessarily being made fully aware of the need for that permission—and is accompanied by collection, aggregation, and storage of detailed personal information and travel histories for millions of noncitizens and U.S. citizens.

The information collected consists of several categories of overlapping but distinct data. First, noncitizen visitors seeking to enter the United States by air or sea without visas, under the Visa

174. See *Terrorist Exploitation of Refugee Programs: Hearing Before the Subcomm. on Counterterrorism and Intelligence of the H. Comm. on Homeland Security*, 112th Cong. 11–12 (2012) (prepared statement of Barbara L. Strack, Chief, Refugee Affairs Division, U.S. Citizenship and Immigration Services); Achraf Farraj, *Refugees and the Biometric Future: The Impact of Biometrics on Refugees and Asylum Seekers*, 42 COLUM. HUM. RTS. L. REV. 891 (2011).

175. ANDORRA BRUNO, CONG. RESEARCH SERV., REFUGEE ADMISSIONS AND RESETTLEMENT POLICY 5–6 (2014); Emily Holland, *Moving the Virtual Border to the Cellular Level: Mandatory DNA Testing and the U.S. Refugee Family Reunification Program*, 99 CALIF. L. REV. 1635 (2011); see also JILL ESBENSHADE, IMMIGR. POL'Y CTR., AN ASSESSMENT OF DNA TESTING FOR AFRICAN REFUGEES, 4 (2010) (analyzing pilot program and raising concerns that “DNA testing in the refugee context may portend required DNA testing in other areas of immigration admissions”).

Waiver Program, must apply online for authorization before commencing their travel. These individuals are required to submit biographic and travel information and to answer questions concerning their eligibility using the Electronic System for Travel Authorization (“ESTA”), and carriers must verify compliance before permitting them to board. ESTA shares this information with the National Counterterrorism Center and automatically screens this information against antiterrorism, immigration control, and criminal law enforcement databases, using ATS and other TECS databases, to determine whether these would-be visitors present threats to aviation security or national security, are of interest to law enforcement, or may be inadmissible for some other reason. Like visas, travel authorizations under ESTA, which are valid for two years, do not establish or guarantee admissibility, and by the same token, individuals who have been denied authorization are directed to U.S. diplomatic posts where consular official may issue visas to those individuals or otherwise resolve the issue.¹⁷⁶

Second, as discussed above, Congress has required air and sea carriers traveling to and from the United States to transmit all passenger and crew manifest information to U.S. officials before departure, including both noncitizens’ and U.S. citizens’ information. Non-U.S.-based air carriers must also submit this information for flights within or overflying the United States.¹⁷⁷ This advance passenger information (“API”) consists of basic personal information

176. 8 U.S.C. § 1187(a)(9)–(11), (g), (h)(3) (2013); U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-11-335, VISA WAIVER PROGRAM: DHS HAS IMPLEMENTED THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION, BUT FURTHER STEPS NEEDED TO ADDRESS POTENTIAL PROGRAM RISKS (2011); DEP’T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION (ESTA) (2008); *see also Statement by Secretary Johnson on Security Enhancements to the Visa Waiver Program*, DEP’T OF HOMELAND SEC. (Nov. 3, 2014), <http://www.dhs.gov/news/2014/11/03/statement-secretary-johnson-security-enhancements-visa-waiver-program> (discussing expansion of biographic and travel information required to be submitted via ESTA). As with individuals who have been issued visas, border inspectors are authorized to make their own, de novo determinations as to whether individuals seeking to enter the United States under the Visa Waiver Program are admissible. 8 U.S.C. §§ 1187(a), 1201(h), 1235(a).

177. 49 U.S.C. § 44909(c)(1)–(2) (2013); Final Rule, Advance Electronic Transmission of Passenger and Crew Manifests for Commercial Aircraft and Vessels, 72 Fed. Reg. 48,320 (Aug. 23, 2007). These advance passenger information sharing requirements also have been extended to private air carriers, and similar information sharing protocols also have been implemented on a voluntary basis with Amtrak and certain private bus carriers. DEP’T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM (APIS) (2008); DEP’T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCED PASSENGER INFORMATION SYSTEM—VOLUNTARY RAIL AND BUS SUBMISSIONS (APIS-VRBS) (2008).

collected from the traveler's passport and other travel documents but also includes information collected from the carrier's own reservations and departure control systems, such as flight or vessel details. API data also includes information collected directly from travelers at check-in, including information on the individual's travel and U.S. destination.¹⁷⁸ Noncitizen travelers who decline to provide this information may be inadmissible, and U.S. citizens who decline to provide this information may be prohibited from traveling by the carrier or subjected to greater scrutiny upon arrival in the United States.¹⁷⁹

Through its Advance Passenger Information System ("APIS"), CBP begins receiving this information in batches as early as seventy-two hours prior to departure and analyzes and compares this information in real time against information in the No Fly and Selectee watchlists generated by the TSDB. When this review is complete, CBP either clears the carrier to issue a boarding pass, instructs the carrier to conduct additional security screening, or directs the carrier not to issue a boarding pass.¹⁸⁰ As discussed above, CBP also stores this information in the BCIS and ADIS databases within TECS and compares it against other government databases to facilitate customs and immigration clearance upon arrival.

Third, Congress and DHS have required international air and sea carriers to transmit passenger name record ("PNR") data to U.S. officials prior to departure to or from the United States, and to give U.S. officials the ability to also access this information directly from airlines' reservation and departure control systems.¹⁸¹ PNR data overlaps with but is broader than API data. Depending on the particular configuration of the carrier's reservations and departure control systems, PNR data can include not only the traveler's biographic data, contact information, and basic travel data, but also detailed information on the individual's travel, including the full itinerary for the trip, transactional details about the reservation (including notations of all changes), payment and billing details,

178. KROUSE & ELIAS, *supra* note 134, at 25.

179. DEP'T OF HOMELAND SEC., PRIVACY OFFICE, *supra* note 47.

180. 19 C.F.R. § 122.49a(b)(1)(ii) (2014); *see* Final Rule, Advance Electronic Transmission of Passenger and Crew Manifests for Commercial Aircraft and Vessels, 72 Fed. Reg. at 48323–24.

181. 49 U.S.C. § 44909(c)(3) (2013); Interim Rule, Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States, 67 Fed. Reg. 42,710, 42,712 (June 25, 2002) (codified at 19 C.F.R. § 122.49d (2014)).

frequent flier program information, baggage and seat information, information about travel companions and other parts of the individual's trip, and comments by reservation systems or travel agents on special issues or requests (such as special meal requests or particular medical needs).¹⁸² CBP stores PNR data in ATS and, as discussed above, compares and analyzes this information against a broad array of government databases in order to assess terrorism-related risks the traveler is deemed to present.¹⁸³

Finally, under TSA's "Secure Flight" program, airlines must send TSA basic biographic information, referred to as "Secure Flight Passenger Data" ("SFPD"), for all passengers traveling by air—including international flights that arrive in, depart from, or overfly the United States and domestic flights within the United States. While overlapping in some respects, the data collection process for Secure Flight differs from CBP's API and PNR data collection processes in both timing and content. When passengers make flight reservations, carriers must request basic biographic information from them as it appears on an approved identification document. Then, seventy-two hours before the scheduled departure time (or at the time of the reservation, for reservations made within seventy-two hours of departure), the carrier must transmit this information to TSA via APIS along with other information in the airline's reservation systems, including itinerary details, PNR record locator, and, if already available to the airline, the traveler's passport information.¹⁸⁴ CBP (for international flights) or TSA (for domestic flights) then compares and analyzes that information against the No Fly and Selectee Lists generated by the TSDB. As with the API process, the airline is either cleared to issue a boarding pass, instructed to conduct additional security screening, or directed not to issue a boarding pass.¹⁸⁵

When flights and vessels arrive in the United States, CBP inspectors compare the information in the arriving passengers' travel documents with the API data transmitted prior to departure and a series of other government databases. Officials now also collect

182. EDWARD HASBROUCK, FREQUENTLY ASKED QUESTIONS ABOUT PNR DATA (2012), <http://hasbrouck.org/IDP/EU-PNR-FAQ.pdf>; Edward Hasbrouck, *What's in a Passenger Name Record (PNR)?*, THE PRACTICAL NOMAD, <http://hasbrouck.org/articles/PNR.html>; see also KROUSE & ELIAS, *supra* note 134, at 26.

183. KROUSE & ELIAS, *supra* note 134, at 9–11.

184. Final Rule, Secure Flight Program, 73 Fed. Reg. 64,018 (Oct. 28, 2008); *Secure Flight: Frequently Asked Questions*, IDENTITY PROJECT, http://papersplease.org/sf_faq.html.

185. Final Rule, Secure Flight Program, 73 Fed. Reg. at 64,019.

biometric data at almost all ports of entry from most categories of noncitizens arriving in the United States, including virtually all individuals arriving by air or sea and many individuals arriving by land.¹⁸⁶ As discussed above, records of all border crossings are recorded in the BCIS database within TECS and, for noncitizens, within ADIS.

4. *Post-Entry Enforcement*

With both direct and indirect immigration enforcement activities increasingly taking place after individuals have entered the United States, as discussed in Part I, surveillance processes and technologies that enable collection, processing, storage, and dissemination of personal information have also proliferated to facilitate those enforcement activities.¹⁸⁷ A number of examples illustrate these developments:

Monitoring and Registration. The NSEERS program initiated in the aftermath of the 2001 attacks, which is discussed above, required Arab and Muslim nonimmigrant men (1) to be fingerprinted and photographed upon arrival in the United States (or to appear for registration if already in the United States), (2) if they remained in the country longer than thirty days, to periodically report for in-person interviews, and (3) to register again when departing the United States.¹⁸⁸ Biometric identifiers collected from these individuals have been enrolled in IDENT, and other personal information and narrative reports of NSEERS interviews—and of the “voluntary” interviews conducted by the FBI have been stored in other government databases.¹⁸⁹ By the end of 2003, officials had collected information on approximately 83,000 registrants, leading to the deportation of almost 14,000 individuals.¹⁹⁰ When the Obama Administration partially suspended NSEERS in 2011, it already had been partially superseded by more general entry-exit tracking

186. Final Rule, Enrollment of Additional Aliens in US-VISIT, 73 Fed. Reg. 77,473 (Dec. 19, 2008); SEGHETTI, *supra* note 49, at 23–24.

187. See *supra* Parts I.B–C.

188. RIGHTS WORKING GROUP, *supra* note 71, at 15–16.

189. CHISHTI ET AL., *supra* note 70, at 18–19, 41; DEP’T OF HOMELAND SEC., OFFICE OF INSPECTOR GEN., INFORMATION SHARING ON FOREIGN NATIONALS: BORDER SECURITY (REDACTED) 4–6, 9–11 (2012).

190. RIGHTS WORKING GROUP, *supra* note 71, at 26–29. While NSEERS remained active until April 2011 and continues to have a number of residual effects, no authoritative data is available concerning the number of individuals affected since 2003. Shoba Sivaprasad Wadhia, *Business as Usual: Immigration and the National Security Exception*, 114 PENN ST. L. REV. 1485, 1507–08 (2010).

mechanisms, but the Administration did not terminate the program altogether or foreclose its future use. Information collected under NSEERS continues to be maintained and used by DHS—for example, by CBP’s Automated Targeting System when making its automated risk assessments.¹⁹¹

Congress also has mandated more extensive ongoing monitoring of international students and exchange visitors, requiring educational institutions to share enrollment status and other personal information on these individuals and their dependents with DHS and expanding the FBI’s ability to obtain student records that otherwise would be protected from disclosure.¹⁹² To implement these mandates, DHS has developed the Student and Exchange Visitor Information System (“SEVIS”), a database system through which schools must regularly report personal information about international students—including their enrollment status, class attendance, changes in majors, disciplinary action, or early graduation—and their dependents.¹⁹³ DHS officials use SEVIS not only to monitor and identify international students who may have fallen out of lawful nonimmigrant status but also to “identify patterns of criminal activity, including terrorism” and to “identify trends and patterns to assist in planning and analyzing risks.”¹⁹⁴

Immigration Policing. Interoperable databases now play a powerful role in federal programs to enlist state and local law enforcement and corrections officers in the identification of potentially deportable noncitizens by enabling automatic, routine, and effectively mandatory immigration status determinations by these officers in the course of their day-to-day responsibilities. Under DHS’s “Secure Communities” program, fingerprints that are recorded and transmitted to the FBI’s

191. System of Records Notice for Automated Targeting System, 77 Fed. Reg. 30,297, 30297–303 (May 22, 2012); Removing Designated Countries From NSEERS, 76 Fed. Reg. 23,830, 23,830–01 (Apr. 28, 2011); RIGHTS WORKING GROUP, *supra* note 71.

192. Enhanced Border Security and Visa Entry Reform Act §§ 501–502, Pub. L. No. 107-153, 116 Stat. 543 (2002); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001 §§ 416, 507, Pub. L. No. 107-56, 115 Stat. 272 (2001); Illegal Immigration Reform and Immigrant Responsibility Act § 641, Pub. L. No. 104-208, 110 Stat. 3009 (1996).

193. Romero, *supra* note 68; see also ALISON SISKIN, CONG. RESEARCH SERV., MONITORING FOREIGN STUDENTS IN THE UNITED STATES: THE STUDENT AND EXCHANGE VISITOR INFORMATION SYSTEM (SEVIS) (2005).

194. U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-04-690, PERFORMANCE OF INFORMATION SYSTEM TO MONITOR FOREIGN STUDENTS AND EXCHANGE VISITORS HAS IMPROVED, BUT ISSUES REMAIN 67 (2004); see also SHANNON R. ANDERSON, BILL OF RIGHTS DEFENSE COMM., TOTAL INFORMATION AWARENESS AND BEYOND: THE DANGERS OF USING DATA MINING TECHNOLOGY TO PREVENT TERRORISM 7–8 (2004).

IAFIS database (to obtain identification and criminal history information as part of the typical post-arrest booking process) are now simultaneously transmitted to DHS for comparison against records in IDENT. If the fingerprints match a record in IDENT—or even if there is no match, but the individual has an unknown or non-U.S. place of birth—the system automatically flags the record for further review. Based on enforcement priorities and other factors, ICE may decide to initiate removal proceedings against the individual and issue a detainer requesting that the state or local agency hold the individual for transfer of custody. A second automated immigration policing program enables automatic identification of suspected immigration law violators by including automatic searches of civil immigration records whenever state and local law enforcement officers search the NCIC to obtain information on criminal history and outstanding warrants on individuals who they encounter. Both programs have been implemented in a manner that makes participation effectively mandatory for states and localities.¹⁹⁵

Immigration Benefits Applications. Just as the State Department does with individuals applying for visas and refugee status from overseas, DHS, through USCIS, collects, stores, analyzes, and disseminates significant amounts of personal information from individuals affirmatively applying for parole, adjustment of status, asylum, employment authorization, lawful permanent resident status, naturalization, and other immigration benefits within the United States. USCIS maintains and tracks benefits applications using its Central Index System, which is able to access over fifty-seven million records concerning the individuals who have applied for these immigration benefits in a variety of different case management database systems.¹⁹⁶ Collection of fingerprints from immigration benefits applicants has become routine, and serious consideration has been given to routine collection of other biometric data, most notably DNA.¹⁹⁷ Officials conduct background checks against a variety of other government databases.¹⁹⁸ USCIS has even used social

195. Kalhan, *supra* note 9, at 1122–31. That said, in practice the precise manner in which that local participation takes place still can vary significantly from jurisdiction to jurisdiction. *Id.* at 1153–54, 1159–62; see generally Ingrid V. Eagly, *Criminal Justice for Noncitizens: An Analysis of Variation in Local Enforcement*, 88 N.Y.U. L. REV. 1126 (2013).

196. DEP'T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE CENTRAL INDEX SYSTEM (2007); see MEISSNER ET AL., *supra* note 5, at 71–72.

197. LYNCH, *supra* note 113, at 6–8.

198. DEP'T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE IMMIGRATION BENEFITS BACKGROUND CHECK SYSTEM 2–4 (2010).

networking platforms to conduct surveillance on individuals seeking to naturalize. The agency has instructed its officials to “friend” petitioners for naturalization and their beneficiaries on social networks in an apparent effort to detect potential grounds upon which those petitions might be denied, such as the failure to meet the legal standard for a genuine marriage.¹⁹⁹

Employment Eligibility Verification. The process by which employers verify whether their new hires are eligible to work in the United States is undergoing a significant transformation with the implementation of USCIS’s E-Verify system. Under this pilot program, which was first authorized and initiated during the 1990s, employers collect personal information from the identification and work authorization documents that employees already must present under the existing, paper-based verification process and submit that information through the online E-Verify system. The system then attempts to match the individual’s data with records contained in databases maintained by DHS, the State Department, and the Social Security Administration (“SSA”) in order to determine whether the individual is authorized to work in the United States. If the system finds a match, then the employer is informed that the individual is authorized to work. If there is no match, or there are discrepancies between the information submitted and the database records, the system will issue a “tentative non-confirmation” and direct the employer to refer the employee to either DHS or SSA to resolve the issue. If the issue is not resolved within eight days, the employer will be informed that the individual is not authorized to work.²⁰⁰

While formally still a pilot program that remains voluntary for most employers, E-Verify has grown extensively in the past ten years due to a series of federal, state, and local mandates. In 2008, the Bush Administration mandated the system’s use by federal contractors and subcontractors, and the Obama Administration has maintained the requirement.²⁰¹ In addition, while some states have sought to limit the system’s use by employers within their jurisdictions, a

199. Jennifer Lynch, *Applying for Citizenship? U.S. Citizenship and Immigration Wants to Be Your “Friend,”* EFF DEEPLINKS (Oct. 12, 2010), <http://www.eff.org/deeplinks/2010/10/applying-citizenship-u-s-citizenship-and>.

200. ANDORRA BRUNO, CONG. RESEARCH SERV., ELECTRONIC EMPLOYMENT ELIGIBILITY VERIFICATION 2–3 (2013); DEP’T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE E-VERIFY PROGRAM 6–7 (2010); U.S. CITIZEN. AND IMMIGR. SERVS., E-VERIFY USER MANUAL FOR EMPLOYERS (2012); Stumpf, *supra* note 130.

201. Final Rule, Employment Eligibility Verification, 73 Fed. Reg. 67651 (Nov. 14, 2008).

growing number of states and localities have mandated its use by various categories of employers.²⁰² Leading reform proposals would dramatically extend the reach of this system—not only by requiring all employers to use E-Verify but also by enhancing the system to incorporate biometric identification mechanisms and, potentially, by making the employment verification system interoperable with other database systems.²⁰³

Public Benefits, Services, and Licenses Eligibility Verification. Somewhat less visibly than some of their other database systems, such as Secure Communities and E-Verify, federal immigration authorities have developed the Systematic Alien Verification for Entitlements (“SAVE”) program, which enables federal, state, and local government agencies to verify immigration status information for individuals applying for an ever-growing variety of public benefits and services.²⁰⁴ Now administered and maintained by USCIS, SAVE was initially authorized by IRCA in 1986 to enable officials to obtain immigration status information from INS in order to determine applicants’ eligibility for certain specified federally funded benefits programs.²⁰⁵ Since then—with significant expansions in the extent to which federal, state, and local authorities have restricted eligibility for services and benefits on the basis of immigration and citizenship status—the ambit of the SAVE program has been extended to

202. LAWLOGIX, E-VERIFY REQUIREMENTS: FEDERAL, STATE, COUNTY, AND MUNICIPAL LEVELS (2013). *But see* United States v. Illinois, No. 07-3261, 2009 WL 662703 (C.D. Ill. March 12, 2009) (discussing and invalidating as preempted Illinois law prohibiting employers from using E-Verify until DHS and SSA systems achieve certain accuracy thresholds).

203. Border Security, Economic Opportunity and Immigration Modernization Act, S. 744, 113th Cong. § 3101(a) (as passed by Senate, June 27, 2013); David Kravets, *Biometric Database of All Adult Americans Hidden in Immigration Reform*, WIRED (May 10, 2013), <http://www.wired.com/threatlevel/2013/05/immigration-reform-dossiers>; *see* Hu, *supra* note 120, at 1509–28.

204. IMMIGRATION POL’Y CTR., THE SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS (SAVE) PROGRAM: A FACT SHEET (2011).

205. Immigration Reform and Control Act of 1986 § 121, Pub. L. No. 99–603, 100 Stat. 3359 (1986). The programs for which these immigration status-based eligibility verifications were initially mandated by IRCA included Aid to Families with Dependent Children, Medicaid, Food Stamps, certain territorial assistance programs administered by the Department of Health and Human Services, the unemployment compensation program administered by the Department of Labor, the Title IV educational assistance program administered by the Department of Education, and certain housing assistance programs administered by the Department of Housing and Urban Development. *Id.*; *see* U.S. CITIZEN. AND IMMIGR. SERVS., SAVE PROGRAM GUIDE 2–3 (2014); DEP’T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS (SAVE) PROGRAM 12 (2011).

encompass a broader range of federal, state, and local benefits, services, licenses, grants, and other programs.²⁰⁶

Over one thousand agencies now access SAVE, including federal, state, and local benefits agencies and state drivers' licenses bureaus. SAVE also is used by agencies that conduct federal security clearances and background investigations on individuals to verify the immigration status of those individuals and their family members, cohabitants, and other affiliates, and by military officials in the course of their recruitment activities.²⁰⁷ To implement the large scale eligibility verification requirements established by the Affordable Care Act, which are discussed above, federal authorities have integrated SAVE with the systems created by the Department of Health and Human Services to operate the exchanges established under the legislation.²⁰⁸

SAVE does not itself furnish any eligibility determinations but rather provides immigration status information from its systems upon which the many federal, state, and local agencies requesting that information make those determinations themselves using their own applicable criteria. Those agencies collect personal information from applicants and other sources and transmit that information to SAVE using an online system. As with E-Verify, the SAVE system then attempts to match the individual's data against a series of government databases that contain over 100 million records, the majority of which are maintained by agencies other than USCIS. If the SAVE system identifies a matching record, it provides the requesting agency with information concerning the individual's immigration status. If it does not find a match, SAVE instructs the agency to take additional steps, in consultation with USCIS officials, to verify the individual's

206. See Illegal Immigration Reform and Immigrant Responsibility Act § 642(c), Pub. L. No. 104-208, 110 Stat. 3009 (1996) (requiring federal immigration authorities to respond to any inquiries from federal, state, and local agencies "seeking to verify or ascertain the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law"); Personal Responsibility and Work Opportunity Reconciliation Act of 1996 §§ 401-402, 411-413, 431-432, 434, Pub. L. No. 104-193, 110 Stat. 2105 (establishing mandatory eligibility restrictions and verification requirements for federal public benefits programs on the basis of immigration and citizenship status and authorizing state governments to adopt alienage-based restrictions and verification requirements for other benefits programs); REAL ID Act of 2005 § 202(c)(3)(C), Pub. L. No. 109-13, Div. B, 119 Stat. 302, 302-23 (2005) (requiring states to use SAVE to verify the immigration status of noncitizens applying for driver's licenses and state-issued identification cards).

207. DEP'T OF HOMELAND SEC., PRIVACY OFFICE, *supra* note 205 at 18.

208. SISKIN & LUNDER, *supra* note 93, at 10-11.

immigration status.²⁰⁹ Recent enhancements to SAVE enable agencies to transmit photographs for comparison against digital photographs in government databases.²¹⁰

Public Health Surveillance. Public health officials have also implemented systems to conduct disease surveillance on noncitizens who have entered the United States. Individuals long have been inadmissible on certain public health-related grounds, and Congress has required individuals seeking admission to undergo medical examinations in their countries of origin before being issued immigrant visas or being admitted as refugees. Individuals seeking to enter as nonimmigrants can be required to undergo medical examinations upon arrival at ports of entry.²¹¹ To implement these inadmissibility provisions and the statutory obligation to prevent communicable diseases from being introduced and transmitted within the United States, the Centers for Disease Control and Prevention has established the Electronic Disease Notification system, which collects and stores health information on these individuals and transmits that health information to state and local public health authorities and refugee resettlement authorities when noncitizens with certain specified health conditions enter their jurisdictions.²¹²

Detention and Removal. Finally, both ICE and the Department of Justice's Executive Office of Immigration Review ("EOIR"), which supervises the immigration courts and the Board of Immigration Appeals, maintain systems to collect, store, analyze, and disseminate information about noncitizens who have been investigated or charged as inadmissible or deportable, booked and placed in removal proceedings, held in detention or alternative forms of custody, and

209. DEP'T OF HOMELAND SEC., PRIVACY OFFICE, *supra* note 198, at 2; DEP'T OF HOMELAND SEC., OFFICE OF INSPECTOR GEN., U.S. CITIZENSHIP AND IMMIGRATION SERVICES SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS PROGRAM ISSUES 4 (2012).

210. DEP'T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT UPDATE FOR THE SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS (SAVE) PROGRAM 2-3 (2013).

211. 8 U.S.C. §§ 1182(a)(1), 1201(d) (2013); RUTH ELLEN WASEM, CONG. RESEARCH SERV., IMMIGRATION POLICIES AND ISSUES ON HEALTH-RELATED GROUNDS FOR EXCLUSION (2011); *see also* Price, *supra* note 93; Muzaffar Chishti, Faye Hipsman & Sarah Pierce, *Ebola Outbreak Rekindles Debate on Restricting Admissions to the United States on Health Grounds*, MIGRATION INFO. SOURCE (Oct. 23, 2014), <http://www.migrationpolicy.org/article/ebola-outbreak-rekindles-debate-restricting-admissions-united-states-health-grounds>.

212. Deborah Lee et al., *Disease Surveillance Among Newly Arriving Refugees and Immigrants—Electronic Disease Notification System, United States, 2009*, MORBIDITY & MORTALITY WKLY. REP., Nov. 15, 2013, at 2; *see also* Wendy K. Mariner, *Mission Creep: Public Health Surveillance and Medical Privacy*, 87 B.U. L. REV. 347 (2007) (discussing issues arising from use of database systems for public health and disease surveillance).

removed from the United States. ICE's Enforcement Integrated Database ("EID"), which officials access using a system referred to as ENFORCE, stores this information in several separate modules. ENFORCE also enables ICE officials to access information in other database systems, such as the FBI's NCIC system and DHS's IDENT database.²¹³ A component in ENFORCE also is used to generate automated risk assessments for individuals when they are booked, which ICE uses to determine whether and under what kinds of circumstances individuals should be detained.²¹⁴ EOIR maintains case management information in its Case Access System for EOIR ("CASE").²¹⁵ These systems have facilitated the significant increases seen in recent years in the number of individuals detained and removed. For example, enrollment in IDENT has enabled expanded use of reinstatement of removal.²¹⁶

III. LEGALIZATION AND THE IMMIGRATION SURVEILLANCE STATE

These broad expansions in the scope of immigration enforcement, together with major investments to construct the technological infrastructure to support those expansions, have given rise to what I described above as the *immigration surveillance state*.²¹⁷ In its current incarnation, the immigration surveillance state has most visibly facilitated a regime of mass detention and deportation. However, as an approach to governance, immigration surveillance runs much deeper, encompassing a broader range of activities that both control and facilitate migration and mobility of both noncitizens and U.S. citizens, both within and outside the United States. Accordingly, in this Part, I explain why comprehensive immigration reform and other legalization proposals, while holding the potential to drastically reduce the number of noncitizens subject to removal from the United States, are not only unlikely to slow or reverse the

213. DONALD KERWIN & SERENA YI-YING LIN, MIGRATION POL'Y INST., IMMIGRATION DETENTION: CAN ICE MEET ITS LEGAL IMPERATIVES AND CASE MANAGEMENT RESPONSIBILITIES? 9–10 (2009).

214. DEP'T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT UPDATE FOR THE ENFORCEMENT INTEGRATED DATABASE RISK CLASSIFICATION ASSESSMENT, ENFORCE ALIEN REMOVAL MODULE, AND CRIME ENTRY SCREEN 3–4 (2012).

215. DEP'T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE OPLA CASE MANAGEMENT SYSTEM 25 (2013).

216. ROSENBLUM, *supra* note 30, at 7 n.45.

217. *See supra* note 111 and accompanying text.

development of the immigration surveillance state but, to the contrary, are likely to consolidate and extend its reach.²¹⁸

To begin with, comprehensive approaches to immigration reform conventionally have been understood to entail a pairing between two sets of objectives: regularization of current undocumented immigrants and increased future immigrant and nonimmigrant flows, on the one hand, along with increased investments in border control and immigration enforcement, on the other.²¹⁹ Accordingly, like IRCA's legalization provisions in 1986, the past decade's leading comprehensive reform proposals—from the Bush Administration's reform principles in 2004, to the bills passed by the Senate in 2006 and 2013, to the Obama Administration's reform principles in 2013, to the reform principles briefly floated by House Republicans in January 2014—all forcefully pledge major investments to expand immigration enforcement activities across all of the many domains in which they now take place, including further investments in the new technologies used to fashion the immigration surveillance state.

However, legalization also reinforces immigration surveillance at an even more basic level. Like other aspects of immigration governance, legalization programs—even if they take the form of straightforward “amnesty” rather than the more demanding “earned legalization” that today's leading proposals contemplate—necessarily require identification, screening, and authorization of individuals to determine whether they meet certain eligibility criteria and to formally confer the legal status that they seek. For example, IRCA's legalization program—which granted permanent residence to individuals meeting the relatively straightforward criteria of having resided in the United States before a specified cutoff date or having performed agricultural work for at least ninety days during the prior year—required applicants to provide documentation establishing

218. Cf. Martin, *supra* note 3, at 526 (arguing that the “one truly indispensable component of viable immigration reform must be steps that will steadily build a stable, during, and functional enforcement system”).

219. MARY GIOVAGNOLI, IMMIGRATION POL'Y CTR., OVERHAULING IMMIGRATION LAW: A BRIEF HISTORY AND BASIC PRINCIPLES OF REFORM (2013); Sheila Jackson Lee, *Why Immigration Reform Requires a Comprehensive Approach That Includes Both Legalization Programs and Provisions to Secure the Border*, 43 HARV. J. ON LEGIS. 267 (2006); JEB BUSH & CLINT BOLICK, IMMIGRATION WARS: FORGING AN AMERICAN SOLUTION (2013). *But see* KEVIN R. JOHNSON, OPENING THE FLOODGATES: WHY AMERICA NEEDS TO RETHINK ITS BORDERS AND IMMIGRATION LAWS 196–97 (2007) (urging reform that combines more open immigration policies with enforcement and border controls “much narrower than the current restrictionist regime”).

their identity, residence, financial responsibility, and proof of employment; to be fingerprinted and photographed; and to appear for an in-person interview.²²⁰

The “earned legalization” approaches contemplated by today’s comprehensive reform proposals are considerably more complex, involving stringent initial eligibility criteria and long probationary periods during which applicants must satisfy a series of continuing obligations to “earn” legal status.²²¹ For example, under the initial eligibility criteria in the Senate’s 2013 reform bill, applicants not only must satisfy a durational residence requirement but also must not have convictions for specified offenses; pay an application fee, a penalty, and any back taxes; submit biometric and biographic data; and successfully complete national security, criminal law, and immigration background checks. After extended periods of time in this provisional status, individuals may adjust to permanent resident status if they continue to satisfy the initial eligibility criteria, successfully complete a second set of background checks, and meet a series of additional prospective criteria, such as obtaining employment, satisfying minimum income requirements, remaining continuously physically present in the United States, registering for the military draft, meeting English language proficiency and civics knowledge requirements, and others.²²²

To implement and monitor compliance with these requirements, authorities invariably will turn to the techniques and technologies of immigration surveillance—collecting, storing, analyzing, and disseminating vast quantities of information on millions of eligible noncitizens, on an ongoing basis, to identify and ascertain who qualifies for legalization and, ultimately, for adjustment to lawful permanent resident status. In a world in which the availability of more information is almost always assumed to be better, the likelihood of long retention periods and secondary use of that data for purposes not contemplated at the time of collection is quite

220. See HING, *supra* note 24, at 166–70 (discussing IRCA’s legalization program and its implementation).

221. COUNCIL ON FOREIGN RELATIONS, REPORT OF THE INDEPENDENT TASK FORCE ON U.S. IMMIGRATION POLICY 77–78 (2009); *cf.* Ayelet Shachar, *Earned Citizenship: Property Lessons for Immigration Reform*, 23 YALE J.L. & HUMAN. 110, 140–41 (2011).

222. Border Security, Economic Opportunity and Immigration Modernization Act, S. 744, 113th Cong. §§ 2101, 2102, 2211, 2212 (as passed by Senate, June 27, 2013).

high.²²³ By definition, not every unauthorized migrant will be able to regularize his or her status. Those who ultimately fall short of these requirements and remain undocumented—an enduring population that, as Michael Wishnie describes, will effectively become “super-undocumented,” even more deeply in the shadows than current undocumented immigrants—will continue to face the entire spectrum of enforcement practices, processes, and penalties that have emerged in recent decades, if not more aggressive and intrusive mechanisms of surveillance and control.²²⁴

Albeit on a comparatively modest scale, the Obama Administration’s Deferred Action for Childhood Arrivals (“DACA”) program offers a glimpse at how immigration reform reinforces the immigration surveillance state.²²⁵ Strictly speaking, DACA involves a categorical but temporary exercise of prosecutorial discretion, but the “DACAmended” status it confers should be understood as a form of quasi-legalization.²²⁶ The program permits unlawfully present noncitizens under the age of thirty-one to request a renewable, two-year period of temporary relief from deportation and employment authorization if they arrived in the United States while below age sixteen; have continuously resided in the United States since June 15, 2007; are currently enrolled in school, graduated from high school or a GED program, or received an honorable U.S. military discharge; have not been convicted of certain specified criminal offenses; and do not otherwise present any threat to national security or public safety.²²⁷

DACA applicants must submit documentation to USCIS establishing their identity and fulfillment of these eligibility criteria.

223. See Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 262 (2013) (“The ethos of our age is ‘the more data, the better.’”).

224. Michael J. Wishnie, *Labor Law After Legalization*, 92 MINN. L. REV. 1446, 1458–61 (2008).

225. See Koh, *supra* note 130, at 1846–51 (describing the “inherently tenuous nature” of the status conferred by DACA).

226. ROBERTO G. GONZALES & VERONICA TERRIQUEZ, IMMIGRATION POL’Y CTR., HOW DACA IS IMPACTING THE LIVES OF THOSE WHO ARE NOW DACAMENTED: PRELIMINARY FINDINGS FROM THE NATIONAL UNDACAMENTED RESEARCH PROJECT (2013); *The Top Ten Benefits Of Being DACA-Mented!*, UNITED WE DREAM, <http://unitedwedream.org/daca-top10/>.

227. Memorandum from Janet Napolitano, Secretary of Homeland Security, to David V. Aguilar, Acting Commissioner, U.S. Customs and Border Protection, et al., *Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children* (June 15, 2012); see Lauren Gilbert, *Obama’s Ruby Slippers: Enforcement Discretion in the Absence of Immigration Reform*, 116 W. VA. L. REV. 255 (2013).

In addition, USCIS collects detailed biographic information and biometrics (photographs, fingerprints, and signatures) from all applicants in order to conduct criminal history and national security background checks against FBI's IAFIS, DHS's TECS, and other government databases, and to enroll individuals into IDENT if their biometric records are not already included.²²⁸ Experts have estimated that as many as 1.8 million individuals could be eligible for DACA, and as of March 2014, over 673,000 DACA applications had been received.²²⁹

Whether as part of comprehensive immigration reform or in some other incarnation, any legalization program that Congress ultimately might adopt would invariably require—on a much larger scale—similar processes of data collection, processing, storage, and dissemination of personal information.²³⁰ While legalization usually is framed in public discourse as a means of advancing justice, compassion, and human dignity, advocates and policymakers increasingly characterize legalization as a means of achieving instrumental objectives closely tied to the logic of immigration surveillance. For example, some legalization advocates emphasize the social harms that arise from a large “underground shadow population” and the benefits legalization would bring by enabling authorities to “learn the names and addresses of the nation’s inhabitants.”²³¹ Especially in the wake of the 2001 attacks, these instrumental arguments are frequently advanced in the name of national security and public safety:

[T]he security dangers of allowing a large, unauthorized population to remain are substantial. Effective homeland security requires that the U.S. government know who is living in this country to the greatest extent possible. It is

228. *Consideration of Deferred Action for Childhood Arrivals (DACA)*, U.S. CITIZEN. AND IMMIGR. SERVS., <http://www.uscis.gov/childhoodarrivals>; DEP'T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT FOR THE DEFERRED ACTION FOR CHILDHOOD ARRIVALS (DACA) 7–8 (2012); DEP'T OF HOMELAND SEC., PRIVACY OFFICE, *supra* note 198; DEP'T OF HOMELAND SEC., PRIVACY OFFICE, PRIVACY IMPACT ASSESSMENT UPDATE FOR THE DEFERRED ACTION FOR CHILDHOOD ARRIVALS (DACA) 2–5 (2014).

229. IMMIGRATION POL'Y CTR., WHO AND WHERE THE DREAMERS ARE, REVISED ESTIMATES (2012); U.S. CITIZEN. AND IMMIGR. SERVS., NUMBER OF I-821D, CONSIDERATION OF DEFERRED ACTION FOR CHILDHOOD ARRIVALS BY FISCAL YEAR, QUARTER, INTAKE, BIOMETRICS AND CASE STATUS: 2012–2014, SECOND QUARTER (2014).

230. DONALD M. KERWIN & LAUREEN LAGLAGARON, MIGRATION POL'Y INST., STRUCTURING AND IMPLEMENTING AN IMMIGRANT LEGALIZATION PROGRAM: REGISTRATION AS THE FIRST STEP (2010).

231. Stephen H. Legomsky, *Portraits of the Undocumented Immigrant: A Dialogue*, 44 GA. L. REV. 65, 101 (2009).

simply not safe to allow so many to live a shadow existence in the country. Efforts at deportation will only drive such people further underground in an effort to evade immigration enforcement, when U.S. security would be better served by making their presence here lawful.²³²

With these pragmatic concerns front and center, the task of making unauthorized noncitizens visible and legible to government authorities invariably becomes a central objective in any legalization scheme.²³³ To that end, the logic, practices, and institutions of immigration surveillance—of identification, screening and authorization, mobility tracking and control, and information sharing—also become critical.

IV. THE CONSEQUENCES OF IMMIGRATION SURVEILLANCE

What happens when technology, surveillance, and information are placed at the heart of immigration governance? In this Part, I identify and discuss several consequences of this transformation, analyzing immigration surveillance within the context of a broader set of developments, extending beyond immigration regulation itself, concerning the role of technology, surveillance, and information in contemporary governance. First, I highlight the ways in which immigration surveillance has deterritorialized the national border for migration and mobility purposes, which complicates and blurs lines of oversight and accountability by dramatically expanding both the actors conducting immigration control activities and the locations where those activities take place. Second, I identify and analyze two sets of concerns arising from these developments that highlight the need for stronger accountability mechanisms: the risks and fallibilities arising from automation and the risks that immigration surveillance systems will later be deployed for secondary purposes not contemplated at the time of implementation. Across all of the many domains in which immigration surveillance takes place, these risks increasingly impose the costs of immigration control upon U.S. citizens and noncitizens with lawful status in the United States.

232. COUNCIL ON FOREIGN RELATIONS, *supra* note 221, at 79.

233. KERWIN & LAGLAGARON, *supra* note 230; Bill Ong Hing, *Misusing Immigration Policies in the Name of Homeland Security*, 6 NEW CENTENNIAL REV. 195, 212–16 (2006); Shachar, *supra* note 221, at 157.

A. *Deterritorializing the Migration Border*

Borders, it is routinely observed, are malleable constructions rather than fixed realities: “less than definite, permeable, and subject to shifts and changes.”²³⁴ As such, to speak of “the border” in the context of immigration governance can be misleading and insufficiently nuanced. While territorial borders have long played a constitutive role in defining nation-state sovereignty under international law, like other kinds of boundaries they can be relevant and important for some purposes but not for others, and in varying degrees.²³⁵ In some contexts, nonterritorial demarcations are more consequential than territorial borders. The significance and meanings given to both territorial and nonterritorial boundaries are legally, politically, socially, economically, and culturally defined, and can evolve and shift over time.²³⁶

The deployment of new technologies and practices of immigration surveillance has accelerated a long-term process of decoupling the territorial border of the United States from what I term its *migration border*: the set of boundary points at which nation-states authorize individuals to enter or be admitted, prevent or allow their entry or admission, or subject them to possible expulsion.²³⁷ Of course, migration borders have never been fully coextensive with territorial borders as a literal matter. Indeed, a longstanding cluster of legal fictions treats individuals as being “at the border” or seeking “entry” when they have been paroled into the United States or arrive at boundary points that, strictly speaking, are well within the country’s territorial limits.²³⁸ Like other nation-states, the United States also has

234. JOHNSON, *supra* note 219, at 7–8; see ANDREAS, *supra* note 24, at 140–42, 151–52; JULIE MOSTOV, *SOFT BORDERS: RETHINKING SOVEREIGNTY AND DEMOCRACY* (2008).

235. KAL RAUSTIALA, *DOES THE CONSTITUTION FOLLOW THE FLAG? THE EVOLUTION OF TERRITORIALITY IN AMERICAN LAW* 5 (2009); Kal Raustiala, *The Geography of Justice*, 73 *FORDHAM L. REV.* 2501, 2508–13 (2005).

236. ANDREAS, *supra* note 24, at 152; SASSEN, *supra* note 17.

237. See Saskia Sassen, *Bordering Capabilities Versus Borders: Implications for National Borders*, 30 *MICH. J. INT’L L.* 567, 568 (2009) (“[T]raditional borders now coexist with a variety of other bordering dynamics and capabilities.”); see also ELSPEETH GUILD, *SECURITY AND MIGRATION IN THE 21ST CENTURY* (2009); SASSEN, *supra* note 17, at 222–76; Ayelet Shachar, *The Shifting Border of Immigration Regulation*, 3 *STAN. J. C.R. & C.L.* 165 (2007).

238. See, e.g., *Almeida-Sanchez v. United States*, 413 U.S. 266, 272–73 (1973) (deeming searches of passengers and cargo upon arrival at an inland international airport to occur at the “functional equivalent” of the border for purposes of Fourth Amendment analysis); *United States v. Ramsey*, 431 U.S. 606, 616–19 (1977) (same); *Leng May Ma v. Barber*, 357 U.S. 185, 187–190 (1958) (deeming arriving noncitizen who has been temporarily paroled into the United States to continue to hold the legal status of an individual “on the threshold of initial entry”); *Shaughnessy v. United States ex rel. Mezei*, 345 U.S. 206, 213–15

long acted extraterritorially to prevent individuals from entering—for example, by interdicting and turning away would-be migrants while they are still traveling to the United States through international waters.²³⁹ Migration boundary points also typically exist within broader zones that often are treated as roughly equivalent, in varying degrees, to the actual boundary points themselves.²⁴⁰ Nevertheless, a powerful and commonplace narrative assumes that migration borders are and should be coextensive with territorial borders—as reflected in the very fact that the doctrinal principles that comprise entry-related legal fictions are understood as “fictions” in the first place rather than simply as doctrinal nuances or complexities.

However, in combination with immense expansions of immigration enforcement activities, immigration surveillance has hastened the detachment of migration borders from territorial borders. On the one hand, the changes in rules and practices for use of drones along the U.S.-Mexico border, visa issuance, the Visa Waiver Program, preinspection and screening of travelers outside the United States, and pre-departure collection and analysis of travelers’ data from international carriers all seek—self-consciously and by design—to push the migration border extraterritorially outward.²⁴¹ This objective long predates the 2001 terrorist attacks. As volumes of cross-border traffic into the United States became considerably larger, officials began to implement extraterritorial screening mechanisms as a means of facilitating more efficient immigration and customs screening when individuals and goods arrived in the United States.²⁴² Since the late 1990s, however, and especially since the 2001 attacks, the expansion of extraterritorial migration and mobility screening mechanisms increasingly has been justified with reference to antiterrorism, national security, and public safety-related concerns—

(1953) (deeming noncitizen to be at the border when seeking entry upon arrival and during subsequent harborage at Ellis Island); Laura J. Arandes, *Life Without Parole: An Immigration Framework Applied to Potentially Indefinite Detention at Guantanamo Bay*, 86 N.Y.U. L. REV. 1046, 1049–62 (2011) (discussing legal significance of “admission,” “entry,” and “parole” under immigration law).

239. *Sale v. Haitian Centers Council, Inc.*, 509 U.S. 155, 158–59 (1993).

240. *E.g.*, Brian Palmer, *What’s Life Like in an Airport Transit Zone?*, SLATE (July 2, 2013), http://www.slate.com/articles/news_and_politics/explainer/2013/07/edward_snowden_has_spent_a_week_in_a_transit_zone_at_moscow_s_airport_what.html; *see* Gerald L. Neuman, *Anomalous Zones*, 48 STAN. L. REV. 1197, 1229–31 (1996).

241. KOSLOWSKI, *supra* note 142, at 3.

242. U.S. GEN. ACCOUNTING OFFICE, *supra* note 38 at 1–6; U.S. GEN. ACCOUNTING OFFICE, GAO/NSIAD-91-6, INTERNATIONAL TRADE: EASING FOREIGN VISITORS’ ARRIVALS AT U.S. AIRPORTS (1991).

as seen in Congress's explicit 2004 finding that "[t]he further away from the borders of the United States that screening occurs, the more security benefits the United States will gain."²⁴³ DHS understands its own mission in precisely these terms: to "push[] our operational borders outward so that our physical borders become our last line of defense and not our first."²⁴⁴

On the other hand, the expansion of both direct and indirect post-entry enforcement simultaneously draws the migration border inward, self-consciously constructing virtual, domestic border checkpoints throughout the country's interior by identifying "events that are necessary for life in a modern society" where it may be possible to "exercise control" over individuals in a manner analogous to the control exercised at the territorial border.²⁴⁵ The particular approaches of these post-entry enforcement initiatives vary considerably, and each one involves a distinct set of public and private actors—including law enforcement and criminal justice officials, but also welfare agencies, public hospitals and health agencies, motor vehicle licensing agencies, private employers, private landlords, and potentially others. Collectively, however, these initiatives establish a kind of immigration panopticism, which eliminates zones in society where immigration status is invisible and irrelevant and puts this large array of public and private actors in the position of identifying individuals and determining immigration status; collecting, analyzing, and storing personal information; screening and identifying potential immigration law violators; and sharing information with federal immigration authorities.²⁴⁶ While these initiatives increase the likelihood of placing many individuals in removal proceedings, proponents place even greater emphasis on their ability to trigger a process they characterize as "self-deportation," which disciplines potentially deportable noncitizens into internalizing the perception that their immigration status is constantly being monitored and,

243. Intelligence Reform and Terrorism Prevention Act of 2004 § 7210(a)(2), Pub. L. No. 108-458, 118 Stat. 3638 (2004). For perspectives predating the 2001 attacks, see U.S. COMMISSION ON NATIONAL SECURITY/21ST CENTURY, ROAD MAP FOR NATIONAL SECURITY: IMPERATIVE FOR CHANGE 12–13 (2001); Flynn, *supra* note 141, at 64.

244. *Fact Sheet: DHS's International Footprint*, DEP'T OF HOMELAND SEC., <http://www.dhs.gov/news/2011/12/02/fact-sheet-dhss-international-footprint> (last updated Dec. 12, 2011); see also Gallya Lahav, *Mobility and Border Security: The U.S. Aviation System, the State, and the Rise of Public-Private Partnerships*, in *POLITICS AT THE AIRPORT* 77, 88 (Mark B. Salter ed., 2008).

245. KRIKORIAN, *supra* note 86, at 5.

246. Kalhan, *supra* note 9, at 1145; see also Huyen Pham, *When Immigration Borders Move*, 61 FLA. L. REV. 1115 (2009) *supra* Part II.A.

ultimately, into both revealing their status in a range of day-to-day settings and conforming to social expectations that they depart the country.²⁴⁷

Far from being a clear, fixed line that is coextensive with the territorial border, the picture of the migration border that emerges is a worldwide, pointillist archipelago of layered boundary points, both fixed and mobile. New immigration surveillance technologies are what make this reconfiguration of the migration border possible. To police this deterritorialized boundary, federal immigration authorities cooperate and coordinate with an enormous number of public and private actors—both within and outside the United States—to collect, analyze, store, and share biometrics and other personal information, to identify individuals, to monitor and control mobility, and in some instances to detain individuals or otherwise restrain their liberty. Interoperable database systems help to create and make possible these broader assemblages, which “integrate and coordinate otherwise discrete surveillance regimes” in both “temporary configurations [and] in more stable structures”—thereby connecting and integrating the vast array of actors and institutions involved in immigration governance.²⁴⁸

This outward and inward projection of the U.S. migration border creates significant challenges to ensure transparency and accountability—particularly as it has been accompanied by the outward and inward projection of the federal government’s policy objectives, priorities, and influence into a variety of other lawmaking and governance settings. As the United States increasingly has emphasized the collection, analysis, management, and dissemination of information about migrants and travelers, it has actively cultivated the development of laws, institutions, and processes—both internationally and domestically—that are conducive to those immigration surveillance objectives.²⁴⁹ Internationally, for example, the United States has strongly advocated within international

247. Kalhan, *supra* note 9, at 1145; Kalhan, *supra* note 1, at 1165–67 (discussing “self-deportation”); see Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297, 317–20 (2003); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1948–52 (2013); MARX, *supra* note 21, at 218–19; MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 200-04 (1977).

248. Kevin D. Haggerty, *Foreword to SURVEILLANCE: POWER, PROBLEMS, AND POLITICS* ix, xvii (Sean P. Hier & Joshua Greenberg eds., 2009); Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRITISH J. SOC. 605, 610–11 (2000); see MEISSNER ET AL., *supra* note 5, at 65.

249. MAGNET, *supra* note 120, at 111–12 (“The border has become the latest North American export.”).

organizations for the implementation of interoperable global standards for machine-readable travel documents, e-passports, and computerized reservations system data formats that facilitate their use in the new information collection and analysis systems that the United States has instituted.²⁵⁰ The expanded collection, storage, and dissemination of API and PNR data by the United States has led to a series of clashes with the European Union—whose data protection regime places greater limits on collection and retention of this data than U.S. law—and ultimately to a series of E.U.-U.S. agreements that acquiesce to U.S. immigration surveillance practices.²⁵¹ Congress also has required countries participating in the Visa Waiver Program to enter into a series of bilateral agreements to share information on individuals traveling to the United States, including antiterrorism watchlists, criminal history records, and lost and stolen passport information.²⁵²

Domestically, the implementation of surveillance technologies in connection with the federal expansion of post-entry enforcement has given rise to a similar dynamic vis-à-vis states and localities.²⁵³ For example, even as the Obama Administration has proactively sought to restrain states from unilaterally undertaking some immigration enforcement activities, such as Arizona's SB 1070, it simultaneously has implemented automated immigration policing programs, such as Secure Communities, that effectively mandate state and local law enforcement collection and information sharing for immigration control purposes—thereby precluding states and localities from making affirmative, calibrated, and negotiated choices about the level of immigration policing assistance they wish to furnish, which they previously had greater latitude to make. As with immigration surveillance initiatives that operate extraterritorially, the technological architecture of these programs shapes the institutional

250. INT'L CIV. AVIATION ORG., MACHINE READABLE TRAVEL DOCUMENTS (MRTDs): HISTORY, INTEROPERABILITY, AND IMPLEMENTATION (2007); *API Guidelines and PNR Reporting Standards*, INT. CIV. AVIATION ORG., <http://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx>; see ACLU, NAKED DATA: HOW THE U.S. IGNORED INTERNATIONAL CONCERNS AND PUSHED FOR RADIO CHIPS IN PASSPORTS WITHOUT SECURITY (2004); MAGNET, *supra* note 120, at 111–12.

251. Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 610–12 (2007); Ian Hosein, *Transforming Travel and Border Controls: Checkpoints in the Open Society*, 22 GOV'T INFO. Q. 594, 599–605 (2005).

252. 8 U.S.C. § 1187(c)(2)(C)–(F) (2012).

253. Kalhan, *supra* note 9, at 1131.

relationships among different actors involved in immigration governance, effecting end runs around affirmative state and local choices and complicating accountability.²⁵⁴

To speak of the migration border's detachment from the territorial border is not to suggest that the territorial border itself has lost significance for migration and mobility purposes. To the contrary, even as the expansion of immigration surveillance has broadened the array of boundary points that comprise the migration border, both extraterritorially and domestically, the territorial border itself remains a site of ever more aggressive immigration surveillance and control. As the massive border fortification investments perennially contemplated by leading immigration reform proposals indicate, demonstrating "toughness" in policing the territorial border continues to carry tremendous expressive and symbolic value for elected officials, quite apart from whether those measures actually succeed in controlling migration.²⁵⁵

Still, an enormous and growing piece of the immigration control action is now found elsewhere. It is not simply the case that the migration border of the United States is "everywhere," although increasingly it is.²⁵⁶ In addition, with the implementation of immigration surveillance technologies—and the resulting projection of influence by the United States over lawmaking and governance, both internationally and domestically—a vast number of actors now contribute to the policing of that migration border at an effectively limitless number of boundary points around the world, which creates significant challenges in promoting transparency, consistency, and accountability among the many actors in that sprawling transnational network.²⁵⁷

B. Automating the Migration Border

With the proliferation of interoperable information systems, monitoring and controlling this deterritorialized migration border has become increasingly automated and semi-automated.²⁵⁸ By itself,

254. For examples and details, see *id.* at 1131–33.

255. Border Security, Economic Opportunity and Immigration Modernization Act, S. 744, 113th Cong. §§ 1101–1123 (as passed by Senate, June 27, 2013); ANDREAS, *supra* note 24, at 145–48.

256. David Lyon, *The Border Is Everywhere: ID Cards, Surveillance and the Other*, in GLOBAL SURVEILLANCE POLICING 66 (Elia Zureik & Mark Salter eds., 2005).

257. See Citron & Pasquale, *supra* note 155.

258. See Citron, *supra* note 19, at 1263–67 (discussing and categorizing different types of automated systems in government programs).

automation is by no means inherently or necessarily harmful.²⁵⁹ To the contrary, at least conceptually automation can help to make government processes more efficient, effective, or fair. For example, the use of machine-readable travel documents and the pre-departure collection of passenger data from international carriers helps to make immigration and customs screening processes upon arrival in the United States more efficient—which, as discussed above, was the original reason why U.S. officials began to collect that information from carriers in the first place. Defenders of CBP’s use of antiterrorism screening mechanisms such as the No Fly List, Selectee List, and ATS emphasize the role of these mechanisms in permitting agency officials to devote scarce resources to more intensive screening of travelers deemed to present the greatest risks.²⁶⁰

In some instances, these automated and semi-automated systems seek to respond directly to concerns arising under their non-automated predecessors. For example, proponents of E-Verify argue that automated employment eligibility verification may reduce opportunities for unlawful discrimination that exist under the existing non-automated employment verification regime.²⁶¹ Similarly, proponents of automated immigration policing programs such as Secure Communities argue that by seeking to eliminate discretionary determinations by state and local police concerning whose immigration status should be investigated and verified, these programs, at least theoretically, reduce the incidence of errors based on police officers’ lack of knowledge of immigration law or invidious exercises of discretion on the basis of race, ethnicity, or national origin.²⁶²

259. See David Lyon, *Introduction*, in *SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK, AND DIGITAL DISCRIMINATION* 1, 2 (David Lyon ed., 2003) (“Surveillance is not itself sinister any more than discrimination is itself damaging.”).

260. See Stodder, *supra* note 130, at 86–88 (“[I]n a busy airport, CBP inspectors cannot send every single person to secondary examination.”).

261. See Stumpf, *supra* note 130, at 398 (examining evidence that E-Verify may reduce “conscious discrimination against employees based on citizenship status, ethnicity, or national origin”).

262. See Adam B. Cox & Eric A. Posner, *Delegation in Immigration Law*, 79 U. CHI. L. REV. 1285, 1344–46 (2012) (arguing that the Secure Communities program’s “more constrained” delegation “eliminates the need for local officials to have any knowledge about immigration law” and “almost certainly produce[s] fewer errors” than previous immigration policing initiatives); see also Anya Bernstein, *The Hidden Costs of Terrorist Watch Lists*, 61 BUFF. L. REV. 461, 485–86 (2013) (suggesting that automated processes could minimize “biases or other weaknesses in reasoning” and “make it easier to spot the effects of cultural predispositions when they conflict with realistic assessments”).

At the same time, automation and semi-automation present significant risks and concerns of their own. Studies indicate that decisionmaking when using computerized systems can be distorted by automation complacency and automation bias, two related phenomena in which individuals place too much trust in the proper functioning of automated systems even when they suspect error or malfunction. When these phenomena are at work, individuals may regard these systems as resistant to error, fail to sufficiently monitor their operation, or overtrust the answers, recommendations, and cues they provide.²⁶³ These risks may be exacerbated with large, complex networks of interoperable information systems like those used for immigration surveillance, since their proper utilization and maintenance present distinct challenges. As Erin Murphy describes, government databases are the “ultimate collaborative projects,” often involving multiple systems and distributed collection, maintenance, access, analysis, and exchange of information among many different actors over extended periods of time.²⁶⁴

In this context, inadequacies in the quality, accuracy, and relevance of information contained in the database systems used for immigration surveillance raise several distinct types of concerns. First, large database systems invariably contain inaccurate, outdated, or irrelevant records, particularly as they grow larger and contain greater quantities of information. Fair information principles emphasize that personal data in government databases should be accurate, complete, and current.²⁶⁵ For decades, however, “immigration authorities have been criticized for maintaining unreliable and inaccurate records and inadequately managing their information systems.”²⁶⁶ While some improvements have been made, these concerns have persisted.

For example, E-Verify regularly issues tentative non-confirmation notices for a significant number of individuals, including both

263. See Citron, *supra* note 19, at 1271–72.

264. See Erin Murphy, *Databases, Doctrine, and Constitutional Criminal Procedure*, 37 *FORDHAM URB. L.J.* 803, 824–25 (2010) (observing that “database” can be a “misleadingly singular” term, given “layers of individuals and objects” involved in their creation, operation, management, and access, often “span[ning] both geographical and temporal boundaries”); see also Bernstein, *supra* note 262, at 481 (“[N]etworked information storage has made it easier for information in one database to be shared with new users, put to new uses, and combined with information from other sources.”); MARX, *supra* note 21, at 210–11.

265. *ORG. FOR ECON. CO-OPERATION & DEV., Doc. C(80)58/FINAL, GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA ¶ 8* (Sept. 23, 1980) [hereinafter *OECD Guidelines*].

266. Kalhan, *supra* note 9, at 1136; see also *NAT’L IMMIGRATION LAW CTR., INS DATA: THE TRACK RECORD* (2003).

noncitizens and U.S. citizens, who in fact are lawfully eligible to work.²⁶⁷ Similarly, a GAO analysis of Secure Communities found that ICE had no record of the criminal arrest charges for more than half of all individuals removed under the program during 2011 and the first half of 2012; other evidence indicates that a significant number of individuals are detained and placed into removal proceedings as a result of the program who ultimately prove not to be deportable.²⁶⁸ More recently, over one million immigrant families have experienced difficulties applying for health care coverage and insurance subsidies under the Affordable Care Act due to problems with verification of their immigration or citizenship status.²⁶⁹

Second, when database systems are made interoperable and accessible to large numbers of actors, erroneous information can propagate widely and quickly and can become even more difficult to correct.²⁷⁰ Outside of immigration agencies, other databases that are relied upon for immigration surveillance purposes suffer from similar data quality problems. For example, despite some recent improvements, criminal history records databases often remain inaccurate, inconsistent across states, and incomplete.²⁷¹ Improper deprivations of liberty based on inaccurate information in these database records remain common.²⁷² Observers also have

267. WESTAT CORP., *supra* note 131; *see also* MARC R. ROSENBLUM, MIGRATION POLICY INST., E-VERIFY: STRENGTHS, WEAKNESSES, AND PROPOSALS FOR REFORM (2011); Stumpf, *supra* note 130, at 399–400.

268. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-708, SECURE COMMUNITIES: CRIMINAL ALIEN REMOVALS INCREASED, BUT TECHNOLOGY PLANNING IMPROVEMENTS NEEDED 22–23 (2012).

269. Letter from AFL-CIO, et al., to Sylvia Mathews Burwell, Secretary of Health and Human Services, *Organizational Sign-On Letter to Improve Access to Health Insurance Under the ACA for Immigrant Families*, July 31, 2014, available at http://ccf.georgetown.edu/wp-content/uploads/2012/04/Advocates-SignOn-Letter-to-Burwell_Immigrant-Barriers-7-29-14.pdf; *see also* DINAH WILEY, IMPLEMENTING THE ACA FOR IMMIGRANT FAMILIES: CONSIDERATIONS AND CHALLENGES (2012); Alex Dobuzinskis & Curtis Skinner, *Obamacare Enrollment by Latinos Hurt by Immigration Law Concerns*, REUTERS (Dec. 18, 2013), <http://reut.rs/1dmy8ee>.

270. *See* JOHN PALFREY & URS GASSER, INTEROP: THE PROMISE AND PERILS OF HIGHLY INTERCONNECTED SYSTEMS 145 (2012) (noting that with increasing interoperability and connectivity among complex systems, “harm can spread like contagion . . . [without] mechanisms to stop it.”); LYNCH, *supra* note 113, at 9.

271. BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, SURVEY OF STATE CRIMINAL HISTORY INFORMATION SYSTEMS, 2010, at 2–8 (2011); *see* James B. Jacobs, *Mass Incarceration and the Proliferation of Criminal Records*, 3 U. ST. THOMAS L.J. 387, 416–18 (2006).

272. *Florence v. Bd. of Chosen Freeholders*, 132 S. Ct. 1510, 1512 (2012); *Arizona v. Evans*, 514 U.S. 1, 27–29 (1995) (Ginsburg, J., dissenting); *United States v. Esquivel-Rios*, 725 F.3d 1231 (10th Cir. 2013); *see* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 46–47 (2004); Murphy, *supra* note 264, at 825.

documented large numbers of concededly innocent individuals whose names have been added to watchlists generated by the TSDB, such as the No Fly List and Selectee List, and inadequate mechanisms exist to remove names of innocent individuals from those lists.²⁷³

Third, contrary to the connotations suggested by the term “database,” the use of these systems does not simply involve the retrieval and reliance of “factual” information, whether accurate or otherwise. To the contrary, as discussed above, much of the information generated by these systems and relied upon by enforcement actors necessarily incorporates analysis, risk assessment, and the exercise of subjective and evaluative human judgments at some stage. Those judgments may have been made directly, such as when individuals are identified for inclusion in the No Fly List, Selectee List, or other watchlists, or indirectly, as with the automated risk assessments made by systems like the ATS and CAPPs, whose evaluations and predictions are generated using algorithms that invariably embed human judgments, assumptions, fallibilities, and potential biases.²⁷⁴ However, in either case, the nature of the data generated and distributed by government database systems—coupled with the opaque nature of the criteria for inclusion—can mask the subjective and evaluative judgments that underlie that information, making it seem more objectively factual to enforcement actors relying upon it than may be warranted.²⁷⁵

Finally, the biometric identification technologies upon which immigration surveillance relies are not foolproof. For example, although automated fingerprint identification systems can be extremely accurate in determining identity, they nevertheless can yield inaccurate results, owing to technological limitations, the quality of fingerprint recording processes, and even the particular demographic groups in which the subjects are members.²⁷⁶ Advanced multimodal biometric identification systems that are currently under development have limitations and fallibilities of their own.²⁷⁷

273. *Ibrahim v. Dep’t of Homeland Sec.*, No. 3:06-cv-00545-WHA (N.D. Cal. Feb. 6, 2014); Shane, *supra* note 134, at 815–19.

274. See Citron & Pasquale, *supra* note 155, 4–6; Citron, *supra* note 19, at 1260–63; Bernstein, *supra* note 262, at 506–07.

275. Bernstein, *supra* note 262, at 486–88.

276. MAGNET, *supra* note 120; see also COLE, *supra* note 22, at 254–58; FROOMKIN & WEINBERG, *supra* note 115, at 4, 7.

277. LYNCH, *supra* note 113, at 10–11; see also GARFINKEL, *supra* note 115, at 37–67; MAGNET, *supra* note 120; Hu, *supra* note 120, at 1534–41.

All of these risks, limitations, and concerns might be more tolerable under circumstances in which database screening processes were merely one step in a fuller investigative process. Indeed, even if it were hypothetically possible for database systems and biometric technologies to be perfectly accurate, consistent, and complete, well-functioning interoperability processes would still depend on competent and effective “human and institutional layers.”²⁷⁸ Officials emphasize that ATS, for example, “does not replace human decision making” but rather is simply a “decision support tool” that “assist[s] the border authorities in targeting scarce inspection resources.”²⁷⁹ Similarly, when E-Verify generates a tentative non-confirmation for a would-be employee or ESTA denies a would-be visitor authorization to travel without a visa, those individuals are given opportunities to resolve the issue in person before any final denial of authorization is issued. Over the long term, improvements in data quality and integrity might help to reduce the percentage of improper deprivations generated by these systems—as already seen to some extent, for example, with E-Verify.²⁸⁰

The nature of immigration surveillance, however, limits the space for these human and institutional layers to function carefully and effectively—and given the enormous scale of immigration surveillance activities, even small error rates can result in very large numbers of individuals facing improper deprivations that are often left unremedied. While intended to eliminate improper discrimination, immigration surveillance mechanisms sometimes merely shift the point at which such discrimination takes place. With E-Verify, for example, employers often decline to hire individuals who receive tentative non-confirmations without properly notifying them—depriving these workers of employment without any opportunity to resolve errors in database records.²⁸¹ Similarly, even as Secure Communities seeks to preclude police from any direct immigration policing role after individuals have been arrested, it empowers police to arrest individuals for the very purpose of booking them and having

278. PALFREY & GASSER, *supra* note 270, at 39–53; see PATO & MILLETT, *supra* note 119, at 19; Murphy, *supra* note 264, at 825.

279. Paul Rosenzweig, *Targeting Terrorists: The Counterrevolution*, 34 WM. MITCHELL L. REV. 5083, 5087–88 (2008); see Stodder, *supra* note 130, at 86–88.

280. WESTAT CORP., *supra* note 131.

281. In some instances, employers also improperly use E-Verify to screen applicants before they have been hired, and then simply avoid hiring or considering applicants for whom the system has generated tentative non-confirmations. ROSENBLUM, *supra* note 267, at 7–8.

their immigration status screened—without regard to whether that arrest leads to any criminal prosecution. Evidence to date suggests that in some jurisdictions, this is precisely what has happened.²⁸² With both of these systems, evidence suggests that these types of errors and deprivations fall disproportionately upon particular communities.²⁸³

Moreover, agencies involved in immigration surveillance are typically subject to limited oversight and deferential (if any) review. Accordingly, those agencies have few incentives to ensure that the records contained in their database systems are accurate, complete, and current. In addition, many of these systems are not governed or meaningfully constrained by any framework statutes. While the Privacy Act of 1974 requires agencies to ensure that government records of personal information are accurate, relevant, timely, and complete, the statute only applies to systems of records about U.S. citizens and lawful permanent residents.²⁸⁴ Moreover, even for records on those categories of individuals, the statute permits agencies to exempt records concerning law enforcement or national security from its coverage.²⁸⁵ While some individuals have filed lawsuits challenging their improper inclusion in these database systems, the lack of transparency concerning the criteria and operations of these systems makes those legal challenges difficult.²⁸⁶ While more accurate database systems would better serve these agencies' own interests, the incentives for immigration control, law enforcement, and national security agencies to devote the resources necessary to ensure the accuracy and integrity of these databases on their own, without external oversight, are limited.²⁸⁷

In short, the combination of database errors, automation-related biases, complex but time-pressured decisionmaking, massive volumes of identification and screening activities, fragmented responsibilities

282. AARTI KOHLI, PETER L. MARKOWITZ & LISA CHAVEZ, *SECURE COMMUNITIES BY THE NUMBERS: AN ANALYSIS OF DEMOGRAPHICS AND DUE PROCESS* 6 (2011).

283. *Id.*; ROSENBLUM, *supra* note 267, at 7–8; Stumpf, *supra* note 130, at 400–01.

284. *See* 5 U.S.C. § 552(a)–(w) (2013).

285. Bernstein, *supra* note 262, at 467–69, 504–06; Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 487 (2013).

286. *Latif v. Holder*, 686 F.3d 1182 (9th Cir. 2012); *Latif v. Holder*, No.-10-Civ.-750, 2014 WL 2871346 (D. Or. June 24, 2014); *Mohamed v. Holder*, 995 F.Supp.2d 520 (E.D. Va. 2014); *Ibrahim v. Dep't of Homeland Sec.*, No.-06-civ.-545 (N.D. Cal. Jan. 14, 2014), ECF No. 682, available at <http://klhn.co/Ibrahim-NDCal-ECF-682>; *see also* First Amended Complaint, *Makowski v. Holder*, No. 12 Civ. 5265 (N.D. Ill. Dec. 17, 2012), ECF No. 45, available at <http://klhn.co/Makowski-NDIll-ECF-45>.

287. Bernstein, *supra* note 262, at 471–73.

among different authorities, and laws and agency incentives that are misaligned with the goal of ensuring data accuracy and integrity can easily result in large numbers of improper denials of immigration-related authorizations in a variety of different contexts. In many instances, these deprivations fall disproportionately on particular groups.²⁸⁸ Especially given the lack of transparency and oversight mechanisms in these systems, the limited procedural protections and access to counsel afforded to noncitizens at all stages of the migration process, and the limited protections for U.S. citizens who are outside the United States or seeking to enter, the consequences of these fallibilities can be significant and difficult to remedy.

C. Data Collection, Retention, and Secondary Use

Quite apart from the accuracy and integrity of data in these systems, immigration surveillance raises the problem of “function creep”: the gradual and sometimes imperceptible expansion of surveillance mechanisms, once in place, for secondary uses beyond those originally intended or contemplated.²⁸⁹ Fair information principles urge limits on the secondary use of information for purposes not specified when collected.²⁹⁰ However, a lengthy list of examples demonstrates that such constraints are often lacking in the first place or difficult to maintain: the proliferation of surveillance camera systems to police a widening array of low level offenses,²⁹¹ the expanding use of online tracking,²⁹² the use of census data and voter lists to facilitate targeting of disfavored individuals or groups,²⁹³ the expansion of DNA databases maintained by law enforcement to

288. KOHLI ET AL., *supra* note 282; cf. Charu A. Chandrasekhar, *Flying While Brown: Federal Civil Rights Remedies to Post-9/11 Airline Racial Profiling of South Asians*, 10 ASIAN L.J. 215 (2003).

289. LAWRENCE LESSIG, CODE: VERSION 2.0, at 210 (2006) (“Systems of surveillance are instituted for one reason; they get used for another.”); see Richard V. Ericson & Kevin D. Haggerty, *The New Politics of Surveillance and Visibility*, in THE NEW POLITICS OF SURVEILLANCE AND VISIBILITY 3, 18–19 (Richard V. Ericson & Kevin D. Haggerty eds., 2006); Gary T. Marx, *Seeing Hazily (But Not Darkly) Through the Lens: Some Recent Empirical Studies of Surveillance Technologies*, 30 LAW & SOC. INQUIRY 339, 385–87 (2005).

290. OECD GUIDELINES, *supra* note 265, ¶¶ 9–10; Solove, *supra* note 112, at 520–22.

291. William Webster, *CCTV Policy in the UK: Reconsidering the Evidence Base*, 6 SURVEILLANCE & SOC’Y 10 (2009).

292. GILLIOM & MONAHAN, *supra* note 4, at 55–63.

293. David Lyon, *Identification, Surveillance and Democracy*, in SURVEILLANCE AND DEMOCRACY 34 (Kevin D. Haggerty & Minas Samatas eds., 2010); William Seltzer & Margo Anderson, *The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses*, 68 SOC. RES. 481 (2001).

encompass rapidly widening categories of individuals and purposes,²⁹⁴ and the repurposing of various categories of identity documents and identification systems.²⁹⁵ Surveillance practices undertaken in the aftermath of the 2001 terrorist attacks have routinely morphed beyond the scope of their original antiterrorism purposes. For example, the “fusion centers” established during the past decade to collect, analyze, and exchange terrorism-related intelligence information among law enforcement agencies almost immediately, and unapologetically, expanded the scope of their activities to encompass ordinary crimes.²⁹⁶

By virtue of the enormous quantities of information that they collect, store, and disseminate—and the rapidly increasing ability to access and share that information among different public and private entities—the systems that comprise the surveillance infrastructure of immigration surveillance are particularly susceptible to secondary uses and function creep. The deployment of immigration surveillance systems and processes has taken place with very few constraints or limitations. Data retention periods for the biometric, biographic, and other personal information in identification systems, travel and mobility control systems, and other databases used for immigration enforcement purposes are exceptionally long, and few limits constrain routine sharing of information among different agencies.

Moreover, as the cost of storing information continues to decrease and the technological capabilities of these systems continue to improve, the number of possible secondary uses for these systems will increase even further—particularly given the premium placed on unconstrained information sharing.²⁹⁷ For example, the most recent

294. Barry Steinhardt, *Privacy and Forensic DNA Data Banks*, in *DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE* 173, 174–75 (David Lazer ed., 2004); Joseph Goldstein, *Police Agencies Are Assembling Records of DNA*, N.Y. TIMES, Jun. 13, 2013, at A1.

295. LYON, *supra* note 4; see also WENDY R. WEISER, JUSTIN LEVITT, CATHERINE WEISS, & SPENCER OVERTON, BRENNAN CTR. FOR JUSTICE, *RESPONSE TO THE REPORT OF THE 2005 COMMISSION ON FEDERAL ELECTION REFORM (2005)* (criticizing proposal to expand use of biometric drivers' licenses and ID cards required by REAL ID Act as a mandatory form of voter identification); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1402 (2001).

296. Monahan & Regan, *supra* note 157, at 303; Citron & Pasquale, *supra* note 155, at 1463–64.

297. Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 YALE L.J. ONLINE 335 (2014); see *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) (“Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive.”).

enhancements to the FBI's identification systems enable collection and storage of unparalleled quantities of biometric and biographic information from a variety of different sources, including multimodal biometric records of fingerprints, multiple photographs, iris scans, palm prints, voice data, and potentially other biometric identifiers along with detailed biographical information. Those systems also will be made fully interoperable with the other identification systems maintained by DHS and the Defense Department that comprise the "biometrics triad," as discussed above.²⁹⁸ In connection with these enhancements, immigration authorities have begun to deploy systems in pilot programs that permit the identification of individuals without any need to review identification documents, using facial recognition and iris recognition technologies that compare biometrics captured in the field with information stored in multiple federal and state government databases.²⁹⁹ Some of these systems also may enable remote identification of individuals without the need to be in their immediate physical proximity.³⁰⁰ Officials also have piloted programs to collect other kinds of biometrics, including DNA from refugees in Africa seeking admission to the United States and noncitizens in immigration detention.³⁰¹

With database systems becoming increasingly sophisticated and interoperable, the pressures for expanded use of the information stored in these systems will continue to mount. At the same time, with few limitations inhibiting them from doing so, immigration authorities might well seek even greater access to database systems maintained and held by federal, state, local, and even private entities for immigration control purposes. However, even as the prospect of

298. *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology, and the Law of the S. Comm. on the Judiciary*, 112th Cong., 102-06 (2012) (written statement of Jennifer Lynch, Electronic Frontier Foundation), available at <http://ssrn.com/abstract=2134497>; Aliya Sternstein, *Feds Significantly Expand the Use of Iris-Recognition Technology*, NEXTEGOV (July 13, 2012), <http://shar.es/Q7y32>; see *supra* notes 159-161 and accompanying text.

299. See Donohue, *supra* note 117, at 440-51; Ali Winston, *Facial Recognition, Once a Battlefield Tool, Lands in San Diego County*, CTR. FOR INVESTIGATIVE REPORTING (Nov. 7, 2013), <http://cironline.org/reports/facial-recognition-once-battlefield-tool-lands-san-diego-county-5502>.

300. Jacob Goodwin, *Iris Recognition Is Being Tested on Illegal Immigrants in McAllen, TX*, GOV'T SEC. NEWS (Aug. 31, 2012), <http://www.gsnmagazine.com/node/27136>; Ginger McCall, *The Face Scan Arrives*, N.Y. TIMES, Aug. 30, 2013, at A19; Jennifer Lynch & Dave Maass, *San Diego Gets in Your Face With New Mobile Identification System*, EFF DEEPLINKS (Nov. 7, 2013), <http://www.eff.org/deeplinks/2013/11/san-diego-gets-your-face-new-mobile-identification-system>.

301. LYNCH, *supra* note 113, at 7-8.

ever-widening uses of these systems highlights the importance of addressing those possibilities before particular surveillance mechanisms are widely implemented, the ability to do so can be elusive—particularly when those mechanisms have been deployed rapidly, with minimal transparency, under vague legal authority, and subject to limited external constraints.³⁰²

V. CONSTRAINING THE IMMIGRATION SURVEILLANCE STATE

With the technologies and processes of the immigration surveillance state becoming a more durable part of the landscape of immigration regulation, much greater attention needs to be given to principles and mechanisms to constrain, inform, and guide their implementation and help limit the reach of the immigration surveillance state.³⁰³ In this Part, I identify and advance these principles and mechanisms. My objective in this Part is not to present a detailed catalog of specific policy recommendations for the many different domains in which immigration surveillance activities now take place. Instead, I aim to highlight principles and approaches, in more general terms, that should be considered across all of these many domains, leaving specific prescriptions about particular initiatives for future work. First, I analyze the traditionally undervalued individual and social interests at stake in the collection, processing, and dissemination of detailed personal information for migration and mobility control purposes. Second, I argue against the persistence of border and immigration exceptionalism, which often results in a degree of deference to immigration surveillance activities that is excessive in relation to those interests. Finally, I highlight the importance of improving transparency, oversight, and accountability mechanisms when implementing these initiatives.

A. *Protecting Information Interests in Migration, Mobility, and Travel*

Immigration surveillance demands reassessment of the interests at stake when personal information and travel history are collected,

302. See Ericson & Haggerty, *supra* note 289, at 18–19 (arguing that function creep is “notoriously difficult to transform into a coherent and successful stakeholder politics”); Marx, *supra* note 285, at 387 (“Asking questions about the process of surveillance creep and possible latent goals should be a central part of any public policy discussion of surveillance *before* it is introduced.”).

303. See BUSH & BOLICK, *supra* note 219, at 54–56 (urging expanded use of surveillance technologies in immigration enforcement, but also advocating “measures protecting individual privacy, requiring immediate correction of false identifications, and setting forth procedures for obtaining and using biometric data”).

maintained, analyzed, and disseminated for purposes related to immigration control and the mechanisms to protect those interests.³⁰⁴ The proliferation of zones where immigration control activities take place—and where detailed information on individuals and their migration and mobility histories is collected and subsequently aggregated, stored, and disseminated—carries a range of social costs.³⁰⁵ While it is entirely appropriate to collect, maintain, and disseminate personal information for immigration control purposes in some contexts and subject to certain constraints, both individuals and society as a whole have legitimate interests in preserving zones in which these immigration surveillance activities do not take place and in making sure that when they do take place those activities are appropriately limited and constrained.

To some extent, those interests are individual interests, stemming from the value of preserving individual anonymity or quasi-anonymity more generally and the individual harms that can result when individuals' migration and mobility are routinely tracked and detailed information is maintained.³⁰⁶ But they also arise from a broader set of social concerns that surveillance and information privacy scholars have increasingly recognized as important. These social interests—for example, preventing coercive or excessive aggregations of unrestrained government power—often have less to do with the particular information being collected in any given instance than with the harms that can arise from the means of surveillance and information management.³⁰⁷ In recent decisions, the Supreme Court has signaled a willingness to give greater weight to these kinds of interests than they have traditionally received.³⁰⁸

304. See Solove, *supra* note 112, at 490–91 (proposing typology of privacy-related problems arising from the collection, storage, analysis, usage, and dissemination of information from data subjects).

305. Kalhan, *supra* note 1; see Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559, 591–93 (1998).

306. See Helen Nissenbaum, *The Meaning of Anonymity in an Information Age*, 15 INFO. SOC'Y 141, 144 (2006); A. Michael Froomkin, *Legal Issues in Anonymity and Pseudonymity*, 15 INFO. SOC'Y 113, 115–16 (1999).

307. Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶¶ 58–70; David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); SOLOVE, *supra* note 272, at 93–101; Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. (forthcoming 2014) (manuscript at 9–13), available at <http://ssrn.com/abstract=2493449>; Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1099–1100 (2006); Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2177 (2003).

308. Riley v. California, 134 S. Ct. 2473 (2014); United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring); *id.* at 957 (Alito, J., concurring).

Vindicating these interests in the context of immigration surveillance therefore requires context-appropriate constraints on the collection, use, storage, and dissemination of personal information for immigration enforcement purposes—including robust limits on retention periods and secondary uses of information that were not originally contemplated. To date, however, exuberance over the potential benefits of interoperable databases and other new technologies has clouded attention to the continued importance of these limits when implementing these systems for migration and mobility control purposes. In an era in which more data is almost always assumed to be better, more information sharing and interconnectivity between database systems is also often assumed to be better as well.³⁰⁹ But as John Palfrey and Urs Gasser have emphasized, “complete interoperability at all times and in all places . . . can introduce new vulnerabilities” and “exacerbate existing problems.” Accordingly, they argue, placing constraints upon information sharing and interoperability and retaining “friction in [the] system” may often be more optimal.³¹⁰

B. Ending Border and Immigration Exceptionalism

Immigration surveillance sits at the intersection of several different doctrines that afford significant deference to government actors in border, migration, and mobility control. Under its border enforcement jurisprudence, the Supreme Court has afforded federal officials considerable latitude to conduct immigration and customs enforcement activities. This deference is strongest at the physical border itself, where the Court has deemed “routine,” suspicionless searches and seizures of individuals and property for purposes of enforcing immigration and customs laws to be per se reasonable, and therefore exempt from the Fourth Amendment’s warrant and probable cause requirements, “simply by virtue of the fact that they occur at the border.”³¹¹ The Court has reached this conclusion with little explanation, often relying on conclusory statements or invocations of history and tradition with little more.³¹² In some instances, the Court has explicitly invoked and tied this “border

309. Citron & Gray, *supra* note 223, at 262.

310. PALFREY & GASSER, *supra* note 270, at 75–76.

311. *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

312. See Paul Rosenzweig, Comment, *Functional Equivalents of the Border, Sovereignty, and the Fourth Amendment*, 52 U. CHI. L. REV. 1119, 1123 (1985) (“Although susceptible to criticism, this historical justification has become the Court’s standard reply to challenges to the border search exception.”).

exception” to the federal government’s power over immigration, which it has long deemed to be plenary. In others, the Court has instead characterized border searches as falling within the categories of exceptions from ordinary Fourth Amendment limits for administrative or “special needs” searches.³¹³

In a world in which the migration border is effectively everywhere, policed by large numbers of actors other than federal immigration officials—and in which immigration surveillance activities reach large numbers of U.S. citizens and noncitizens with lawful immigration status—the justifications for such sweeping deference become more difficult to maintain. The categories of potential deprivations that can result from immigration surveillance activities have multiplied drastically beyond the simple ability to enter and remain in the United States. With the expansion of the domains of enforcement and the tools of immigration surveillance, these enforcement activities can place restrictions on the rights to international and domestic travel, employment, education, social service benefits, and freedom from physical restraint in both the criminal justice and immigration enforcement processes. As discussed above, the powerful tools of immigration surveillance create significant risks of erroneous deprivations and are easily susceptible for uses beyond those originally contemplated when implemented.

Courts have slowly begun to recognize that significant interests are at stake in immigration surveillance activities for both noncitizens and U.S. citizens.³¹⁴ However, these interests have continued to be given insufficient weight by Congress, which has exempted records of most noncitizens from the Privacy Act, and the executive branch, which has invoked the Act’s exemptions from its coverage for databases used for law enforcement and national security purposes. Narrowing these exemptions in the Act’s coverage would enable these interests to be given the weight that they deserve, and ensure that any

313. *Compare* Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973) (citing Chae Chan Ping v. United States, 130 U.S. 581, 603–04 (1889)) *with* United States v. Montoya de Hernandez, 473 U.S. 531, 538–40 (1985); *see* Kalhan, *supra* note 1, at 1190–1205.

314. *See* Latif v. Holder, 686 F.3d 1182 (9th Cir. 2012); Ibrahim v. Dep’t of Homeland Sec., 669 F.3d 983 (9th Cir. 2012); American Academy of Religion v. Napolitano, 573 F.3d 115 (2d Cir. 2009); Latif v. Holder, No. 10 Civ. 750, 2014 WL 2871346 (D.Or. June 24, 2014); Ibrahim v. Dep’t of Homeland Sec., No. 06 Civ. 545 (N.D. Cal. Jan. 14, 2014), ECF No. 682 (findings of fact, conclusions of law, and order for relief), *available at* <http://klhn.co/Ibrahim-NDCal-ECF-682>; Mohamed v. Holder, 995 F.Supp.2d 520 (E.D. Va. 2014); *see also* First Amended Complaint, Makowski v. Holder, No. 12 Civ. 5265 (N.D. Ill. Dec. 17, 2012), ECF No. 45, *available at* <http://klhn.co/Makowski-NDIll-ECF-45>.

countervailing government interests are recognized and given effect only when supported by reasoned justifications.

C. Transparency, Oversight, and Due Process

Finally, immigration surveillance demands greater attention to transparency, oversight, and accountability. Whether programmatically or in the context of individual adjudications, immigration agencies, although improving in some ways, have long suffered from major transparency and accountability deficits.³¹⁵ Those deficits are amply evident in immigration surveillance initiatives and have been exacerbated by the blurred lines created by the deterritorialized migration border. Ensuring greater transparency, oversight, and due process requires responses at a number of different levels.

First, a major contributing factor to the lack of sufficient transparency, oversight, and accountability has been the lack of sufficiently concrete or detailed legal authority to support and guide such major and complicated initiatives. No framework statutes govern or constrain immigration surveillance activities, which, as discussed above, also fall outside of the limited privacy protections available under the Privacy Act. This lack of a statutory framework governing surveillance activities that implicate privacy interests in migration, mobility, and travel data stands in marked contrast to other areas, such as communications and financial services, in which government access, storage, and dissemination of personal information have long been governed and constrained by framework statutes.³¹⁶

Whether coming from Congress, the executive branch, or both acting together, accountability and oversight of immigration surveillance would be better served by a more detailed, coherent legal framework governing immigration surveillance activities and opportunities for greater public engagement with those rules. As the

315. Chacón, *supra* note 7; Sklansky, *supra* note 7, at 212–21; Serena Hoy, *The Other Detainees*, LEGAL AFF., Sept.–Oct. 2004, at 58; Andrew Becker, *Ousted Chief Accuses Border Agency of Shooting Cover-Ups, Corruption*, CTR. FOR INVESTIGATIVE REPORTING (Aug. 14, 2014), <http://beta.cironline.org/reports/ousted-chief-accuses-border-agency-of-shooting-cover-ups-corruption>.

316. *E.g.*, Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994); Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, Title XI, 92 Stat. 3641, 3697–3710 (1978); *see* Hasbrouck, *supra* note 148, at 4; Kalhan, *supra* note 1, at 1210–11. While critics have questioned the adequacy of some of these statutory constraints, no comparable statutory framework governs or constrains most immigration surveillance activities to any meaningful extent.

Markle Foundation has emphasized, new national security information sharing initiatives demand privacy and security protections that “address the hard questions [such as secondary use and redress] . . . as opposed to existing policies that state that agencies must comply with the law without providing guidance on how to do so.”³¹⁷ These observations hold true across the full range of initiatives in which immigration surveillance activities take place and will only become more relevant as authorities continue to incorporate, upgrade, and integrate technology-based surveillance mechanisms in other aspects of immigration governance.

Second, individual opportunities to redress harms arising from immigration surveillance activities, whether administrative or judicial in nature, can still play an important role—not only in remedying those individual harms, but also in creating incentives for DHS and other actors to ensure that information maintained in their database systems is accurate and complete.³¹⁸ Current redress mechanisms, however, do not give sufficient opportunities for individuals to remedy improper deprivations. While courts have begun to fill this gap, more robust and regularized redress mechanisms at the administrative level would create additional incentives for the authorities involved in immigration control to ensure the accuracy and integrity of their data.

Finally, immigration surveillance demands more attention to forms of structural oversight. Because of the necessarily opaque manner in which database systems and automated decisionmaking mechanisms often function—and the ways in which multiple actors are involved in their operation over extended periods of time—oversight of these systems can be particularly difficult in the context of individual cases.³¹⁹ This is undoubtedly more true in the immigration enforcement system, which has traditionally been ill-equipped to supervise investigatory practices.³²⁰ Given the limitations in the ability of individual redress mechanisms to fully ensure proper

317. ZOE BAIRD BUDINGER & JEFFREY H. SMITH, MARKLE FOUND., TEN YEARS AFTER 9/11: A STATUS REPORT ON INFORMATION SHARING 7 (2011) (urging the federal government also to “find ways to publically discuss the legal authorities associated with data collection, sharing, and use . . . in order to ensure public trust in the policies and adequate oversight”); see Balkin, *supra* note 4, at 21; Joel R. Reidenberg, *The Data Surveillance State in the United States and Europe*, 49 WAKE FOREST L. REV. 583, 606–08 (2014).

318. See *Herring v. United States*, 555 U.S. 135, 148–57 (2009) (Ginsburg, J., dissenting); *Arizona v. Evans*, 514 U.S. 1, 22–23 (1994) (Stevens, J., dissenting).

319. Murphy, *supra* note 264, at 826–29, 831–32; see Frank Pasquale, *Restoring Transparency to Automated Authority*, 9 J. TELECOMM. & HIGH TECH. L. 235, 235–39, 250–54 (2011).

320. See Chacón, *supra* note 77, at 1603–19.

oversight of database systems, these systems raise the stakes in making sure that structural oversight mechanisms operate effectively.³²¹ Especially as immigration surveillance integrates the institutions of immigration control with each other and with the institutions of other domains, the blurred lines of accountability among different institutions make accountability difficult; the implementation of automated immigration surveillance initiatives only blurs those lines further.³²²

VI. CONCLUSION

Technology, as Erin Murphy has explained, “alters—rather than just mechanizes—the relationship between the individual and the state.”³²³ With the introduction of new surveillance and dataveillance technologies, the traditional relationships between individuals and the institutions of immigration control are being reconfigured in fundamental ways for both noncitizens and U.S. citizens alike. And yet, compared to other aspects of the expansion of immigration enforcement, these shifts in migration and mobility surveillance have garnered exceedingly little attention, analysis, or concern—even as vigorous debates about surveillance and dataveillance by public and private institutions have emerged in other settings.

These shifts have not simply contributed to a regime of mass enforcement, in which hundreds of thousands of noncitizens have faced detention and deportation. More fundamentally, the evolution of immigration enforcement institutions, practices, and meanings has also contributed to a more basic transformation of the nature of immigration governance—with implications for noncitizens and U.S. citizens alike. By recounting and analyzing this transformation and its consequences, this Article highlights the need for scholars, advocates, policymakers, and other observers to devote greater attention and scrutiny to the onset of the immigration surveillance state and its rapid integration into the broader national surveillance state.

321. See Citron & Pasquale, *supra* note 155, at 1470–93 (proposing mechanisms of “network accountability” as means of ensuring proper oversight of fusion centers); Murphy, *supra* note 264, at 826–29 (emphasizing importance of “structural oversight” to ensure the integrity and proper use of database systems); see also Bernstein, *supra* note 262; Anjali Dalal, *Shadow Administrative Constitutionalism and the Creation of Surveillance Culture*, 2014 MICH. ST. L. REV. 59, 118–36.

322. Sklansky, *supra* note 7, at 212–21.

323. Murphy, *supra* note 16, at 145.