Biometric ID Cybersurveillance

MARGARET HU*

The implementation of a universal digitalized biometric ID system risks normalizing and integrating mass cybersurveillance into the daily lives of ordinary citizens. ID documents such as driver's licenses in some states and all U.S. passports are now implanted with radio frequency identification (RFID) technology. In recent proposals, Congress has considered implementing a digitalized biometric identification card—such as a biometric-based, "high-tech" Social Security Card—which may eventually lead to the development of a universal multimodal biometric database (e.g., the collection of the digital photos, fingerprints, iris scans, and/or DNA of all citizens and noncitizens). Such "high-tech" IDs, once merged with GPS-RFID tracking technology, would facilitate exponentially a convergence of cybersurveillance-body tracking and data surveillance, or dataveillance-biographical tracking. Yet, the existing Fourth Amendment jurisprudence is tethered to a "reasonable expectation of privacy" test

---

* Visiting Assistant Professor, Duke Law School. I deeply appreciate the helpful comments from and conversations with those who have generously taken the time to help me with this work, including Jane Bahnson, Jack Balkin, Bill Banks, Kate Bartlett, Jennifer Behrens, Stuart Benjamin, Joseph Blocher, Jamie Boyle, Dru Brenner-Beck, Guy Charles, Bobby Chesney, Jack Chin, Geoff Corn, Michael Dreeben, Charlie Dunlap, Mary Dudziak, Nita Farahany, Laurel Fredrickson, Michael Froomkin, Susan Ginsburg, Linda Greenhouse, Chris Griffin, Lisa Griffin, Amos Guiora, Mitu Gulati, Lucas Guttentag, Keith Guzik, Larry Helfer, John Inazu, Jennifer Jenkins, Christine Jolls, Trina Jones, Fred Kameny, Margot Kaminski, Suzanne Katzenstein, Jj Kidder, Steve Leckar, Ron Lee, Maggie Lemos, Marc Miller, Steve Miskinis, Steve Morrison, Lise Nelson, Dana Norvell, Jeff Powell, Jed Purdy, Arti Rai, Jayesh Rathod, Paul Rosenzweig, Sarah Schroth, Neil Siegel, Scott Silliman, David Sklansky, Balfour Smith, John Szmer, Phil Telfeyan, Dan Tichenor, Shoba Wadhia, John Whitehead, Michael Wishnie, Benjamin Wittes, Ernie Young, and apologies to anyone whom I may have inadvertently omitted. I am also grateful for the feedback received from participants at the Information Society Project's Ideas Lunch, hosted at Yale Law; the Duke Law Spring Faculty Workshop; the National Security Law Faculty Workshop, jointly hosted by the University of Texas and South Texas College of Law; the surveillance and society panel discussion at the Law and Society Annual Conference in Honolulu, Hawaii; the domestic terrorism panel discussion at the Law, Ethics, and National Security (LENS) Conference hosted at Duke Law; the Emerging Immigration Law Scholars Conference, hosted by the Washington College of Law at American University; the "Politics of Surveillance" symposium, hosted by the Wayne Morse Center for Law and Politics at the University of Oregon School of Law; the constitutional law panel discussion at the North Carolina Political Science Association Conference, hosted by UNC Charlotte; and the emerging technologies and society discussion at the Young Leaders Conference in Genoa, Italy, hosted by the Council for the United States and Italy. This research was made possible with the generous support of Dean David Levi and the Duke Law Dean's Office, including Tia Barnes, Curt Bradley, and Liz Gustafson. Finally, I would like to thank Russell Caleb Chaplain and the *Indiana Law Journal* staff for their editorial care, and Chase Anderson, Lauren Bugg, Julie Coleman, Brittany Edwards-Franklin, Jacob Hanger, Benjamin Holt, Richard Hu, Hassan Kanu, Bryan Leitch, Kristi Lundstrom, Eric Mattingly, and James Pearce for their research assistance. All errors and omissions are my own.

that does not appear to restrain the comprehensive, suspicionless amassing of databases that concern the biometric data, movements, activities, and other personally identifiable information of individuals.

In this Article, I initiate a project to explore the constitutional and other legal consequences of big data cybersurveillance generally and mass biometric dataveillance in particular. This Article focuses on how biometric data is increasingly incorporated into identity management systems through bureaucratized cybersurveillance or the normalization of cybersurveillance through the daily course of business and integrated forms of governance.

INTRODUCTION

After the terrorist attacks of September 11, 2001, policymakers questioned whether identity management[1] tools and systems were based upon outdated

1. The U.S. Department of Homeland Security (DHS) offers this definition of identity management:

> Identity Management (IdM) is a broad administrative area that deals with identifying and managing individuals within a government, state, local, public, or private sector network or enterprise. In addition, authentication and authorization to access resources such as facilities or, sensitive data within that

technologies that would fail to keep us secure.[2] Biometric data[3] technologies and systems have been proposed as a solution.[4] Biometric-based identity management systems are now being recommended to augment or supersede existing identity verification tools which include passports, driver's licenses, and Social Security Cards. Because biometric data is a unique signifier, it is perceived to be the most

---

system are managed by associating user rights, entitlements, and privileges with the established identity.

Identity Management and Data Privacy Technologies Project, CYBER SEC. RESEARCH & DEV. CTR., http://www.cyber.st.dhs.gov/idmdp/. For an overview of identity management as a policy concept, see Lucy L. Thomson, *Critical Issues in Identity Management—Challenges for Homeland Security*, 47 JURIMETRICS J. 335 (2007).

2. The 9/11 Commission Report, for example, emphasized the need to incorporate biometric data into identity management tools and systems in order to augment border security and national security objectives. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 385–92 (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf ("Linking biometric passports to good data systems and decisionmaking is a fundamental goal.").

3. Biometrics is "[t]he science of automatic identification or identity verification of individuals using physiological or behavioral characteristics." JOHN R. VACCA, BIOMETRIC TECHNOLOGIES AND VERIFICATION SYSTEMS 589 (2007). Numerous scholars and experts have explored the science and application of biometrics and the consequences of this emerging technology. *See, e.g.*, Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407 (2012); JENNIFER LYNCH, FROM FINGERPRINTS TO DNA: BIOMETRIC DATA COLLECTION IN U.S. IMMIGRANT COMMUNITIES AND BEYOND (2012); A. MICHAEL FROOMKIN & JONATHAN WEINBERG, CHIEF JUSTICE EARL WARREN INST. ON LAW & SOC. POLICY, HARD TO BELIEVE: THE HIGH COST OF A BIOMETRIC IDENTITY CARD (2012), *available at* http://www.law.berkeley.edu/files/Believe_Report_Final.pdf; KELLY A. GATES, OUR BIOMETRIC FUTURE: FACIAL RECOGNITION TECHNOLOGY AND THE CULTURE OF SURVEILLANCE (2011); ANIL K. JAIN, ARUN A. ROSS, KARTHIK NANDAKUMAR, INTRODUCTION TO BIOMETRICS (2011); SHOSHANA AMIELLE MAGNET, WHEN BIOMETRICS FAIL: GENDER, RACE, AND THE TECHNOLOGY OF IDENTITY (2011); BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES (Joseph N. Pato & Lynette I. Millett eds., 2010) [hereinafter BIOMETRIC RECOGNITION]; DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 118–36 (2007); VACCA, *supra*; ROBERT O'HARROW, JR., NO PLACE TO HIDE 157–89 (2005); Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 25 HASTINGS COMM. & ENT. L.J. 653 (2003); U.S. GEN. ACCOUNTING OFFICE, GAO-03-174, TECHNOLOGY ASSESSMENT: USING BIOMETRICS FOR BORDER SECURITY (2002) [hereinafter GAO TECHNOLOGY ASSESSMENT], *available at* http://www.gao.gov/assets/160/157313.pdf; SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 37–67 (2000).

4. *See, e.g.*, GATES, *supra* note 3, at 1–2 ("The suggestion that an automated facial recognition system may have helped avert the September 11 terrorist attacks was perhaps the most ambitious claim circulating about biometric identification technologies in the aftermath of the catastrophe."); JAIN ET AL., *supra* note 3, at vii ("[T]he deployment of biometric systems has been gaining momentum over the last two decades in both public and private sectors. These developments have been fueled in part by recent [post-9/11] government mandates stipulating the use of biometrics for ensuring reliable delivery of various services.").

reliable and fraud-resistant form of identification data.[5] Some examples of biometric data include digital photos, fingerprint and iris scans, and DNA.[6] This Article explores how these post-9/11 concerns have placed an emphasis on expanding the biometric ID cybersurveillance capacities of the government. I examine how these cybersurveillance capacities are expanding through technological advances, the increasing bureaucratization of surveillance, and the broadening scope of identity management systems. Specifically, I contend that emerging biometric cybersurveillance technologies, and mass biometric data collection and database screening, are adding an entirely new and unprecedented dimension to day-to-day bureaucratized surveillance.[7]

To place the identity management phenomenon within its historical context, it is useful to note that identity cards[8] and other forms of identity registration[9] have

---

5. *See infra* Part III.C (describing some of the challenges of biometrics as a solution to identity management system vulnerabilities); Bruce Schneier, *Biometrics*, SCHNEIER ON SEC. BLOG (Jan. 8, 2009), http://www.schneier.com/blog/archives/2009/01/biometrics.html ("[B]iometrics are easy to steal. . . . Biometrics are unique identifiers, but they're not secrets.").

6. In the criminal justice context, in particular, scholars are increasingly examining the consequences of the collection of biometric data, new forensic techniques, and biometric technologies, including the surveillance capacities of these new techniques and technologies. *See, e.g.*, David H. Kaye, *A Fourth Amendment Theory for Arrestee DNA and Other Biometric Databases*, 15 U. PA. J. CONST. L. 1095 (2013); Elizabeth E. Joh, *DNA Theft: Recognizing the Crime of Nonconsensual Genetic Collection and Testing*, 91 B.U. L. REV. 665 (2011); Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CALIF. L. REV. 721 (2007). Other scholars specifically focus their scholarship on a growing predominance of behavioral genetics and the use of neuroscience evidence in the criminal justice system. *See, e.g.*, Nita A. Farahany, *Incriminating Thoughts*, 64 STAN. L. REV. 351 (2012) [hereinafter Farahany, *Incriminating Thoughts*]; Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239 (2012) [hereinafter Farahany, *Searching Secrets*].

7. Multiple scholars have researched the intersection of biometric identification technologies and post-9/11 government surveillance. *See, e.g.*, Lior Jacob Strahilevitz, *Signaling Exhaustion and Perfect Exclusion*, 10 J. ON TELECOMM. & HIGH TECH. L. 321 (2012); David Lyon, *Biometrics, Identification and Surveillance*, 22 BIOETHICS 499 (2008); Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321 (2008); GLOBAL SURVEILLANCE AND POLICING: BORDERS, SECURITY, IDENTITY (Elia Zureik & Mark B. Salter eds., 2005); Elia Zureik & Karen Hindle, *Governance, Security and Technology: The Case of Biometrics*, 73 STUD. POL. ECON. 113 (2004).

8. For a discussion of what documents comprise identity cards and the surveillance consequences of identity documents, see generally DAVID LYON, IDENTIFYING CITIZENS: ID CARDS AS SURVEILLANCE (2009); PLAYING THE IDENTITY CARD: SURVEILLANCE, SECURITY AND IDENTIFICATION IN GLOBAL PERSPECTIVE (Colin J. Bennett & David Lyon eds., 2008). For an overview of the legal and policy implications of recently adopted and recently proposed digitalized identification systems, including privacy issues, see, for example, JIM HARPER, IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD (2006); LAWRENCE LESSIG, CODE VERSION 2.0, at 45–54, 68–70 (2006); PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006); Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 HARV. J.L. & TECH. 319 (2002).

enabled bureaucratized surveillance[10] for more than 200 years.[11] Bureaucratized surveillance is unlike traditional notions of foreign intelligence-type spying for the purposes of strategic defense. Bureaucratized surveillance integrates the mass tracking of ordinary citizens into forms of governance that are normalized and routine.[12] This routinized surveillance is implemented by administrative agencies, or their private sector delegates[13] and security or surveillance assemblages,[14] during

---

9. *See, e.g.*, DOCUMENTING INDIVIDUAL IDENTITY: THE DEVELOPMENT OF STATE PRACTICES IN THE MODERN WORLD (Jane Caplan & John Torpey eds., 2001) (discussing the historical genesis of identity documentation and the transnational nature of identity registration protocols across nation states); JOHN TORPEY, THE INVENTION OF THE PASSPORT: SURVEILLANCE, CITIZENSHIP AND THE STATE (2000) (arguing that modern governments have monopolized the legitimacy of human movement, as well as the conferral and denial of rights and penalties, through the construction of identification systems such as the passport). For additional historical perspectives on identity registration and national identification systems, and proposals for a digitalized ID system in the United States, see generally NATIONAL IDENTIFICATION SYSTEMS: ESSAYS IN OPPOSITION (Carl Watner & Wendy McElroy eds., 2004); JOSEPH W. EATON, CARD-CARRYING AMERICANS: PRIVACY, SECURITY, AND THE NATIONAL ID CARD DEBATE (1986).

10. *See, e.g.*, GATES, *supra* note 3, at 5 (asserting that "scholars maintain that, while late capitalist societies may not precisely mirror Orwell's vision, computerization is nevertheless enabling significant advancements in institutionalized forms of surveillance"); LYON, *supra* note 3, at 74–75 (contending that new forms of surveillance are "'file-based' or bureaucratic surveillance" and elaborating that "modern surveillance methods are rationalized using accounting methods and *file-based* coordination" (emphasis in original)); *see also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004) (describing the manner in which modern privacy violations occur as a result of corporate and bureaucratic action).

11. *See* CRAIG ROBERTSON, THE PASSPORT IN AMERICA: THE HISTORY OF A DOCUMENT 26 (2010) ("By 1782 the passport, although not a required document, was sufficiently recognized that the Continental Congress gave the recently created Department of Foreign Affairs [renamed the Department of State] the responsibility to issue passports in the name of the United States.").

12. *See, e.g.*, GATES, *supra* note 3, at 13 (describing how a "system of standardized documents, archives, and administrative procedures for the management of individual identities itself displaced the more personal and informal forms of trust and recognition characteristic of smaller-scale forms of social organization. The aim of a documentary regime of verification was to assign each individual an official identity that could be verified in repeated transactions with the state and other institutions."); Jane Caplan, *'This or That Particular Person': Protocols of Identification in Nineteenth-Century Europe*, *in* DOCUMENTING INDIVIDUAL IDENTITY, *supra* note 9, at 49, 51; LYON, *supra* note 3, at 80–84.

13. Several scholars have examined the manner in which immigration screening (e.g., inspection of identity and immigration documents or immigration database screening—forms of bureaucratized surveillance and bureaucratized cybersurveillance, respectively) is increasingly privatized or delegated by the federal and state governments to private entities (e.g., employers, landlords, doctors, and transportation companies). *See, e.g.*, Margaret Hu, *Reverse-Commandeering*, 46 U.C. DAVIS L. REV. 535 (2012); Stephen Lee, *Private Immigration Screening in the Workplace*, 61 STAN. L. REV. 1103 (2009); Huyen Pham, *The Private Enforcement of Immigration Laws*, 96 GEO. L.J. 777 (2008). This delegation parallels a movement to delegate and outsource domestic and foreign intelligence gathering activities to the private sector as well. *See, e.g.*, DANA PRIEST & WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE 176–201 (2011).

the daily course of business. Thus, technological advances recently incorporated into the development of typical identity registration methods—such as driver's licenses, passports, and Social Security Cards and Social Security Numbers—are in the process of transforming bureaucratized surveillance by adding a "cybersurveillance"[15] component and data surveillance, or "dataveillance,"[16] component. The term "biometric ID cybersurveillance"[17] describes how recently introduced forms of identity registration and identity processing—such as digitalized ID cards and "cardless" ID systems such as biometric ID databases or smartphones—facilitate a convergence of cybersurveillance-body tracking and dataveillance-biographical tracking.

In other words, contemporary cybersurveillance technologies are merging with bureaucratized surveillance to create "bureaucratized cybersurveillance."[18] This

---

14. LYON, *supra* note 3, at 4 ("Using personal data, techniques derived from military, administrative, employment, policing and consumer practices combine[d] to create a complex matrix of power; a surveillance assemblage."); *see also* Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRIT. J. SOC. 605 (2000).

15. LESSIG, *supra* note 8, at 209 (describing cybersurveillance or "digital surveillance" as "the process by which some form of human activity is analyzed by a computer according to some specified rule. . . . [T]he critical feature in each [case of surveillance] is that a computer is sorting data for some follow-up review by some human.").

16. Roger Clarke is attributed with first introducing the term "dataveillance" into academic discourse. *See* Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498 (1988). Clarke describes dataveillance as the systematic monitoring or investigation of people's actions, activities, or communications through the application of information technology. *Id.*; *see also* LYON, *supra* note 3, at 16 ("Being much cheaper than direct physical or electronic surveillance [dataveillance] enables the watching of more people or populations, because economic constraints to surveillance are reduced. Dataveillance also automates surveillance. Classically, government bureaucracies have been most interested in gathering such data . . . ."); MARTIN KUHN, FEDERAL DATAVEILLANCE: IMPLICATIONS FOR CONSTITUTIONAL PRIVACY PROTECTIONS (2007) (examining constitutional implications of "knowledge discovery in databases" (KDD applications) through dataveillance).

17. *See, e.g.*, GATES, *supra* note 3, at 14 ("The aim of biometric identification technologies—like optical fingerprinting, iris scanning, and voice recognition—is to bind identity to the body using digital representations of unique body parts, or, in the case of voice printing, by capturing, digitizing, and analyzing the sounds that the body produces."); Lyon, *supra* note 7, at 500 ("The electronic information infrastructures that permit the processing of our personal data depend on identification documents and protocols to mediate between individuals and the organizations with which we relate. The employee authenticates her identity with an access card to enter the workplace, the traveler shows a passport to board a plane, and the patient produces a health card to prove eligibility for medical services at the hospital. Without the card, and the databases on which it depends, identity cannot now be verified. Telling your story no longer suffices. It is displaying your card that counts.").

18. *See, e.g.*, GATES, *supra* note 3, at 13 ("These official forms of bureaucratic identification cobbled together a set of existing and already mediated markers of identity—such as names, addresses, signatures, and photographs—to create a more stable and standardized form of identity that could be verified via the very bureaucratic apparatus that constitutes that identity. In short, our seemingly self-evident 'official identities' are in reality a product of bureaucratization and a relatively recent historical construction, and

merger provides a vehicle for normalizing the general populace's acquiescence to experimental and emerging biometric ID cybersurveillance techniques since they now integrate with otherwise traditional forms of identity registration and identity confirmation protocols.[19] Digitalized biometric IDs, for example, illustrate how such newly emerging technologies can risk normalizing and integrating mass cybersurveillance into the daily lives of ordinary citizens. ID documents such as driver's licenses in some states and all U.S. passports are now implanted with radio frequency identification (RFID) technology. In recent proposals, Congress has considered implementing a digitalized biometric identification card—such as a biometric-based, "high-tech" Social Security Card—which may eventually lead to the development of a universal multimodal biometric database. Such a database would potentially require the collection of, for instance, the digital photos, fingerprints, iris scans, and/or DNA of all citizens and noncitizens. Such "high-tech" IDs, once merged with GPS-RFID tracking technology, could facilitate a convergence of 24/7 body tracking and 360° biographical tracking.

Yet, the existing Fourth Amendment jurisprudence is tethered to a "reasonable expectation of privacy" test[20] that does not appear to restrain the comprehensive, suspicionless amassing of databases that concern the biometric data, movements, activities, and other personally identifiable information of individuals.[21] At the same time, most scholars agree that the Fourth Amendment should protect ordinary citizens from mass, suspicionless surveillance[22] and cybersurveillance "fishing expeditions" by the government.[23] Any attempt to grapple with the consequences of modern cybersurveillance, therefore, should attempt to delineate how surveillance is administratively and technologically implemented through increasingly normalized mechanisms of identity tracking. Consequently, it is necessary to consider what role, if any, the Fourth Amendment will play in restraining a rapidly

---

considerable effort has gone into designing systems that can produce and reproduce these identities." (footnote omitted)).

19. *See id.* at 5 (explaining the experimental nature of biometric ID technologies, noting that "[a]lthough developers are making incremental improvements in algorithms and other dimensions of software and hardware development, so far these technologies do not work very well outside constrained settings"); *see also* BIOMETRIC RECOGNITION, *supra* note 3, at viii–ix (discussing experimental nature of technologies).

20. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

21. *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007); Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 11 (Jeffrey Rosen & Benjamin Wittes eds., 2011); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

22. *See, e.g.*, Benjamin Wittes, *Databuse: Digital Privacy and the Mosaic*, GOVERNANCE STUDIES AT BROOKINGS INSTITUTION (Apr. 1, 2011), http://www.brookings.edu/research/papers/2011/04/01-databuse-wittes; JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2001).

23. *See, e.g.*, Solove, *supra* note 21, at 1107 ("[B]y obtaining private sector records, the government can conduct the type of 'fishing expeditions' that the Framers feared." (citing LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 158 (1999); Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse Than the Disease*, 68 S. CAL. L. REV. 1, 9 (1994))).

evolving bureaucratized cybersurveillance movement that now constitutes what some scholars have described as the post-9/11 "national surveillance state."[24]

In order to fully grasp the constitutional and other developing legal consequences of these programs, however, it is necessary to first examine the ways in which cybersurveillance policies and dataveillance technologies are now rapidly unfolding in nearly invisible ways. Specifically, in this Article, I focus on how digitalized biometric IDs could facilitate the convergence of cybersurveillance-body tracking and dataveillance-biographical tracking through a single, automated, centralized system. As a threshold matter, I attempt to illustrate exactly how identity management systems are becoming increasingly integrated into our daily lives. This Article describes identity management policy initiatives and the emerging surveillance technologies they harness.[25] In this Article, I initiate a project to explore the constitutional and other legal implications of a network of bureaucratized cybersurveillance programs and technologies associated with digitalized biometric IDs and identity management systems. Explaining the identity management phenomenon—and the potential surveillance capacities facilitated by the phenomenon—is in itself a descriptive effort that involves a certain amount of technical detail. Consequently, this Article is descriptive by necessity. I reserve for future scholarship more theoretical and prescriptive approaches to this topic.

This Article proceeds in four parts. In Part I, I explain how digitalized biometric IDs can facilitate not only geolocational tracking, but also biometric, behavioral, and biographical tracking. I further describe how identity management systems are providing the policy rationale to push for the expansion of an effective way to "manage," "secure," and "verify" identity. Part II explains how and why the federal

---

24. *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008); Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489 (2006).

25. As an attempt to trace out the broad contours of bureaucratized cybersurveillance and biometric ID cybersurveillance as it is unfolding in this moment, I resort to multiple tables in the Article. For the sake of accessibility and to capture the breadth of the phenomenon, the tables are gross simplifications. Thus, this method, concededly, communicates only the roughest sketch of programs and technologies that are extraordinarily complex. For example, the tables may use terms such as "Technology," "Program," and "Entity." These terms are imprecise. Sometimes a "Technology" is placed in the "Program" column, and vice versa, for ease of description and simplified communication. I attempt to define each briefly here as they are used in the tables. "Technology" characterizes specific information technologies, devices, software, mass analytics tools, etc., that can be put in the service of programs. "Program" refers to the implementation of technologies that serve a specific governmental purpose or policy objective, for example, identity management, or serve a specific legislative, regulatory, or executive mandate, such as E-Verify. "Entity" is a broad term that sometimes encompasses a technology developer or marketer; federal, state, or local administrative agency; a delegated user, such as a private corporation; or others tasked with utilizing or implementing the technology or program. In addition, because it is too cumbersome to list out all of the potential entities implicated for any particular program or technology, often a specific named "Entity" was selected for illustrative purposes, usually based upon which entity appeared to be the most salient at that juncture. An appendix of acronyms and key words is also provided at the conclusion of this Article.

government is taking steps toward the adoption of a digitalized national identification system based upon the development of a universal biometric database. Recent comprehensive immigration reform efforts are particularly instructive in this examination. Part III provides an overview of how biometric ID data is collected and how biometric matching technologies operate. In Part IV, I map out how bureaucratized surveillance is now being transformed at the dawn of big data and mass dataveillance through bureaucratized cybersurveillance. I conclude that biometric ID cybersurveillance will enable the execution of identity management systems in nearly invisible ways through digital means, including mass data collection and tracking, database screening, and data analysis.

I. DIGITALIZED BIOMETRIC IDS AND IDENTITY MANAGEMENT SYSTEMS

The proposal of a digitalized biometric national ID, or centralized, biometric-based identity verification system, is still just that: simply a proposal. The reality of a universal digitalized biometric national ID system, particularly a "cardless" system,[26] however, is not remote. The technologies, laws, and policies that would support it are currently operative. It is a proposal with political resonance in that it mobilizes a political and cultural desire for a certain level of homeland security. Especially pronounced after 9/11, there is a deep political incentive in identifying a method that will assist in the control of our nation's borders and in the regulation of immigration policy and migration flows.

Specifically, since 9/11, as a method to address complex social challenges and as a policy prescription for immigration enforcement, crime control, and counterterrorism, there has been a push to expand technological solutions that can more accurately identify and classify individuals with the minimum level of physical intrusiveness.[27] Digitalized IDs and digitalized identity management systems have been proposed to meet these goals. They are structured to verify or secure identity, analyze ID data, and conduct identification assessments.[28] These bureaucratized cybersurveillance technologies execute surveillance through data- and database-driven methodologies.[29] These methodologies are facilitated by an

---

26. *See, e.g.*, Jim Harper, *The New—Cardless!—National ID*, CATO AT LIBERTY BLOG (June 1, 2011, 3:57 PM), http://www.cato.org/blog/new-cardless-national-id.

27. *See, e.g.*, Donohue, *supra* note 3, at 425–51, 529–33.

28. With the advent of a digitalized civilization and Internet culture, scholars have contemplated how modern technologies impact identity construction, identity traceability, and digital identity registration protocols. *See, e.g.*, LESSIG, *supra* note 8, at 45–54, 68–70; JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 175–84 (2005).

29. Biometric databases, particularly DNA databases, are increasingly relied upon for a variety of criminal law purposes, including "DNA trawling" or "DNA fishing" for prosecution and conviction, as well as using DNA databases for genetic profiling to assess any predictive or diagnostic value. *See, e.g.*, David H. Kaye, *Please, Let's Bury the Junk: The CODIS Loci and the Revelation of Private Information*, 102 NW. U. L. REV. COLLOQUY 70 (2007); David H. Kaye, *Rounding Up the Usual Suspects: A Legal and Logical Analysis of DNA Trawling Cases*, 87 N.C. L. REV. 425 (2009) (discussing how prosecutors are identifying a defendant by "fishing through a database of DNA types to find a match"); Andrea Roth, *Safety in Numbers? Deciding When DNA Alone Is Enough To Convict*, 85

exponential proliferation of digitalized biometric ID programs and emerging identity management technologies.[30]

These systems, programs, and technologies rely upon the mass analytical tools and the cybersurveillance technologies of big data[31] and dataveillance.[32] In recent years, data-driven surveillance technology has developed in two ways: (1) comprehensive geolocational cybersurveillance, or 24/7 surveillance of the body; and (2) comprehensive dataveillance, or 360° surveillance of the biography[33]—amassing as much information as possible on an individual's personal identity and history through data collection and data mining[34] as well as data classification and analysis. Post-9/11 policies are driving the development of programs that combine these two methods. Newly emerging digitalized forms of identification—such as e-Passports, "high-tech" Social Security Cards, and smartphones—that aim to replace traditional paper-based identity documents, now or in the near future, may consolidate 24/7 body tracking with 360° biographical tracking.

A. Digitalized Biometric Data

Biometric technologies go hand in hand with identity management systems under a wide range of post-9/11 policymaking efforts.[35] For example, recent

---

N.Y.U. L. REV. 1130 (2010).

30. *See supra* note 6.

31. *See, e.g.*, VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013); Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63 (2012).

32. *See, e.g.*, Clarke, *supra* note 16, at 502–05.

33. Executives of Acxiom, one of the largest consumer data mining companies in the nation, have acknowledged in media reports that their approach is a "360-degree view" on consumers. Natasha Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES, June 16, 2012, *available at* http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.

34. *See, e.g.*, Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435 (2008); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317 (2008); Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343 (2008). For a history on databases and overview of historical attempts to secure database privacy, see generally GARFINKEL, *supra* note 3.

35. *See* JAIN ET AL., *supra* note 3, at vii (observing multiple post-9/11 identity management programs have mandated "the use of biometrics": "the Enhanced Border Security and Visa Entry Reform Act of 2002 . . . mandated the use of biometrics in the issue of U.S. visas"; "the US-VISIT program (United States Visitor and Immigration Status Indicator Technology) that validates the travel documents of foreign visitors to the United States based on fingerprints"; "[t]he International Civil Aviation Organization (ICAO) has unanimously recommended that its member States use Machine Readable Travel Documents (MRTDs) that incorporate at least the face biometric (some combination of face, fingerprint and iris can also be used) for purposes of verifying the identity of the passport holder"); *id.* at 1–2 (suggesting that biometrics have the potential to enable the technological realization of more accurate identity management systems on a mass scale). Identity management as a policy prescription is a broad umbrella that may include multiple goals:

proponents of comprehensive immigration reform legislation and legislation proposing the mandatory expansion of E-Verify[36]—an Internet-driven identity database screening program—have previously debated how and why a "high-tech, biometric identification card" may be needed "to improve E-Verify."[37] In previous debates, specifically, it had been proposed that the government should adopt a "high-tech Social Security Card" that would resemble a credit card.[38] Policymakers over the past decade, in fact, have argued that a universal digitalized biometric national ID system is needed to increase border security and control immigration.[39] Thus, a push to create a biometric-based and digitalized "high-tech Social Security

---

> Identity management plays a critical role in a number of applications. Examples of such applications include regulating international border crossings, restricting physical access to important facilities like nuclear plants or airports, controlling logical access to shared [computerized and digitalized] resources and information, performing remote financial transactions, or distributing social welfare benefits.

Id. at 1; *see also* IDMANAGEMENT.GOV, http://www.idmanagement.gov; BIOMETRICS IDENTITY MANAGEMENT AGENCY, http://www.biometrics.dod.mil/.

36. For an overview of E-Verify and some of the legal implications of the E-Verify program, see Juliet P. Stumpf, *Getting to Work: Why Nobody Cares About E-Verify (And Why They Should)*, 2 U.C. IRVINE L. REV. 381 (2012).

37. Michael D. Shear & Ashley Parker, *Senators' Plan Alters Waiting Periods for Immigration*, N.Y. TIMES, March 18, 2013, at A11, *available at* http://www.nytimes.com/2013/03/18/us/politics/senate-groups-immigration-plan-would-alter-waiting-periods.html ("The bipartisan group of eight senators is also still debating how to improve E-Verify, the system that employers use to check the immigration status of their workers. A high-tech, biometric identification card was deemed too costly; instead, the group is considering an enhanced E-Verify system that would allow employers to use photographs to identify job applicants and would let workers provide answers to security questions to help prove their legal work status."). Media reports have explained that members of the Senate, in recent discussions and negotiations on comprehensive immigration reform, decided the adoption of the card may be prohibitively expensive. Therefore, it appears that recent discussions have been focused on how to add both a biometric ID verification protocol (digital photo screening) as well as a biographical ID verification protocol (personally identifiable data as "security questions") into the E-Verify system, rather than adopt a biometric ID card system. *Id.* In the version of the bill that was released by the Senate on April 16, 2013, however, Title III includes $1 billion in funding for the Social Security Administration to implement a "high-tech" Social Security Card and requires the DHS Secretary to explore the feasibility of a biometric-based employment authorization document. *See infra* note 192.

38. *See, e.g.*, Charles E. Schumer & Lindsey O. Graham, Op-Ed., *The Right Way to Mend Immigration*, WASH. POST, Mar. 19, 2010, at A23 (although the Senators do not state explicitly that the card would resemble a credit card, they discuss the need to implement a "high-tech" Social Security Card that would allow "swiping the card through a machine" which suggests the card would function similarly to a credit card); *see also* FROOMKIN & WEINBERG, *supra* note 3.

39. *See, e.g.*, GAO TECHNOLOGY ASSESSMENT, *supra* note 3. "Congress and the 9/11 Commission called for increased use of biometrics, and the White House created a cabinet-level subcommittee to coordinate policy to deploy biometric technology across many federal agencies." U.S. DEP'T OF HOMELAND SEC., ENHANCING SECURITY THROUGH BIOMETRIC IDENTIFICATION 3 (2008), *available at* http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_biometrics_brochure_english.pdf; *see also* Alan M. Dershowitz, *Why Fear National ID Cards?*, N.Y. TIMES, Oct. 13, 2001, at 23.

Card" has been gaining momentum. This can be seen in the use of the word "biometric" on at least 24 separate instances in a proposed comprehensive immigration reform bill,[40] discussed below. This policy trend signals the potential for future development of a universal biometric database for national ID and identity registration purposes.

At the outset, however, it is important to note the distinction between biometric data that is used in a small data context and biometric data that is used in a big data context. In the big data cybersurveillance and dataveillance context, biometric data is not collected and analyzed in an individualized way as it would be in a small data context. For instance, the data is not collected and assessed to serve a specific criminal law purpose in a forensic evidence context.[41] Rather, new technologies allow for biometric data to be harvested and used for big data analysis and identity management purposes, for criminals and noncriminals alike. In other words, mass biometric data collection and analysis facilitates mass identity registration and suspicionless mass tracking.[42]

Table 1 describes various types of biometric data that can be utilized for identification purposes and for the purposes of identity assessment.

40. *See infra* Table 6.

41. VACCA, *supra* note 3, at 244 ("DNA identification is mainly used in forensics . . . or more precisely, in forensics investigation.").

42. GATES, *supra* note 3, at 15–16 ("[D]igital biometric identification represents the latest in a long line of efforts to stabilize and standardize identification systems [by mass individuation]. . . . Mass individuation is also a modern governmental strategy for security provision and population management, a social regulatory model that involves knowing in precise detail the identity of each member of the population in order to differentiate individuals according to variable levels of access, privilege, and risk.").

Table 1. Digitalized Biometric Data[43]

	Emerging Biometric Technologies	Experimental Biometric Technologies	Speculative Biometric Technologies
Description	"Biometric verification technologies such as face, finger, hand, iris, and speaker [voice] recognition are commercially available today and are already coming into wide use."[44] These technologies have not been fully tested.	Biometric recognition and verification technologies that are in the earliest stages of testing and "that are being studied and developed."[45]	Speculative technologies are attempting to transform biometric data, including transient data, into information with predictive value and other value.[46] Testing is either nonexistent or at nascent stages.

43. Based upon a review of research on the status of specific biometric technologies, including stages of testing, I have classified various biometric technologies as "Emerging," "Experimental," and "Speculative." Experts and researchers generally categorize biometric technologies within classifications that reflect levels of commercial availability and stages of technological development. *See, e.g.*, GAO TECHNOLOGY ASSESSMENT, *supra* note 3, at 136 (distinguishing between "biometric technologies currently deployed, currently available but not yet deployed, or in development that could be deployed in the foreseeable future"); VACCA, *supra* note 3, at 27–39 (distinguishing between "Leading Biometric Technologies" that are "more widely deployed" and "Biometric Technologies Under Development" that are still under study). Most experts appear to agree, however, that biometric technologies are emerging and experimental, and they acknowledge that none have been fully tested for identity management purposes. *See, e.g.*, BIOMETRIC RECOGNITION, *supra* note 3, at 4 ("Many gaps exist in our understanding of the nature and extent of distinctiveness and stability of biometric traits across individuals and groups."); VACCA, *supra* note 3, at 45 ("While biometric technology is currently available and is used in a variety of applications, questions remain regarding the technical and operational effectiveness of biometric technologies in large-scale applications."); GAO TECHNOLOGY ASSESSMENT, *supra* note 3, at 58–67 (explaining the "[l]ack of [a]pplications-[d]ependent [e]valuations" that study the impact of biometric data usage in real-life contexts and summarizing studies showing "[s]usceptibility [of biometric technologies] to [d]eception"); GARFINKEL, *supra* note 3, at 55 ("Despite their apparent accuracy, neither fingerprints nor DNA samples are suitable for identifying individuals on a day-to-day basis."). In contrast, the usage of biometric data for forensic purposes has undergone more rigorous testing and has been tested over several decades. *See, e.g.*, GARFINKEL, *supra* note 3, at 59 (asserting that biometric recognition and verification technologies have not been subjected to the same scientific peer review process as that required of DNA fingerprinting).

44. VACCA, *supra* note 3, at 11.

45. *Id.* at 32.

46. *See infra* note 128 and accompanying text; *infra* Part I.B.3; *see also* MAYER-SCHÖNBERGER & CUKIER, *supra* note 31, at 157–63 (discussing FAST within context of predictive policing).

Examples	Facial Recognition,[47] Fingerprints,[48] Hand Geometry,[49] Iris Scans,[50] Speaker [Voice] Recognition[51]	DNA,[52] Brainwave Patterns[53] and Neural Fingerprinting,[54] Blood Pulse,[55] Gait,[56] Hand and Foot Dominance,[57] Palm Prints,[58] Hormones,[59] Wrist Veins and Vein Patterns,[60] Grip Recognition,[61] Eyebrow Shape,[62] Ear Shape,[63] Skeletal Bone Scan,[64] Knee Cap Analysis,[65] Sweat Pores Analysis,[66] Body Odor,[67] Body Salinity (Salt) Level Identification,[68] Skin Luminescence (Level of Light Refraction),[69] Skin Print (Epidermis Patterns)[70]	Breathing Rates,[71] Pupil Dilation,[72] Eye Movement,[73] Voice Pitch and Variation,[74] Perspiration,[75] Temperature,[76] Facial Expression[77]

47. VACCA, *supra* note 3, at 13.
48. *Id.*
49. *Id.*
50. *Id.* at 13.
51. *Id.*
52. DNA is generally not considered an established biometric data verification technology for several reasons. For example,

> DNA differs from standard biometrics in several ways. It compares actual samples rather than templates generated from samples. Also, because not all stages of DNA comparison are automated, the comparison cannot be made in real time. DNA's use for identification is currently limited to forensic applications. The technology is many years away from any other kind of implementation and will be very intrusive.

GAO TECHNOLOGY ASSESSMENT, *supra* note 3, at 51; *see also* VACCA, *supra* note 3, at 32.
53. Farahany, *Searching Secrets*, *supra* note 6, at 1281 & n.222.
54. *Id.* at 1275, 1287–88.
55. VACCA, *supra* note 3, at 32.
56. *Id.*
57. *Id.* at 32, 37.
58. *Id.* at 187.
59. Donohue, *supra* note 3, at 415.
60. VACCA, *supra* note 3, at 32–33.
61. *Id.* at 32, 34.

B. Identity Management Systems

Bureaucratized cybersurveillance and biometric ID cybersurveillance encompass identity management systems[78] that utilize geolocational, biometric, and biographical data. Specifically, identity management is a policy prescription. It relies upon identity verification, identity determination, and/or identity inference systems to regulate access to places or things. It also serves broader population tracking and screening goals for government policymaking purposes.[79] The prescription relies upon experimental technologies and emerging methodologies. As such, its efficacy is uncertain and the systems have not been fully tested.

Yet, the increasing availability of these emerging cybersurveillance and dataveillance technologies has allowed for the rapid and dramatic expansion of identity management systems since 9/11. These technologies utilize data collection and mining, database screening, and data analysis to reach identity management

---

62. YUJIE DONG & DAMON L. WOODARD, EYEBROW SHAPE-BASED FEATURES FOR BIOMETRIC RECOGNITION AND GENDER CLASSIFICATION: A FEASIBILITY STUDY (2011), *available at* http://www.csis.pace.edu/~ctappert/dps/IJCB2011/papers/133.pdf.

63. VACCA, *supra* note 3, at 203.

64. Mathew J. Schwartz, *Skeletal Scans Explored for Crime Fighting*, INFORMATIONWEEK (Aug. 26, 2010, 1:07 PM), http://www.informationweek.com/software/information-management/skeletal-scans-explored-for-crime-fighti/227100041.

65. Sara Gates, *Knee Scan Identification: MRIs May Be Better Way to ID Travelers, Study Suggests*, HUFFINGTON POST (Jan. 25, 2013, 12:36 PM), http://www.huffingtonpost.com/2013/01/25/kneecap-scans-identification-biometric-id_n_2543042.html.

66. VACCA, *supra* note 3, at 32, 34.

67. *Id.* at 32, 35.

68. *Id.* at 32–33.

69. *Id.* at 32, 36.

70. O'HARROW, *supra* note 3, at 186.

71. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST)/PASSIVE METHODS FOR PRECISION BEHAVIORAL SCREENING 5 (2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast-a.pdf [hereinafter Privacy Impact Assessment for FAST (2011)].

72. Pam Benson, *Will Airports Screen for Body Signals? Researchers Hope So*, CNN.COM (Oct. 7, 2009), http://edition.cnn.com/2009/TECH/10/06/security.screening/index.html.

73. Privacy Impact Assessment for FAST (2011), *supra* note 71, at 3.

74. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST) PROJECT 4 (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf [hereinafter Privacy Impact Assessment for FAST (2008)].

75. *See, e.g.*, Allison Barrie, *Homeland Security Detects Terrorist Threats by Reading Your Mind*, FOX NEWS (Sept. 23, 2008), http://www.foxnews.com/story/0,2933,426485,00.html.

76. Privacy Impact Assessment for FAST (2011), *supra* note 71, at 3.

77. Privacy Impact Assessment for FAST (2008), *supra* note 74, at 4.

78. Identity management systems utilize different techniques that are based upon what you have (e.g., identity cards and Social Security Numbers), what you know (e.g., passwords), and/or what you are (e.g., biometric data). *See* VACCA, *supra* note 3, at xvi.

79. *See supra* notes 4, 39.

determinations. Increasingly, these identity determinations are utilized to restrict access to specific rights and privileges, such as the right to fly ("No-Fly List"), the right to work (E-Verify), and the right to vote (Help America Vote Act of 2002 (HAVA)). Identity management programs are also implemented to assist the government in taking action against certain individuals, such as determining who should be detained and deported (Secure Communities (S-COMM) and Future Attribute Screening Technology (FAST)).

The programs can operate at multiple levels and are not mutually exclusive to each category. Therefore, an identity verification or determination program, such as E-Verify or S-COMM, can also serve identity inference objectives. Some identity management systems are not yet biometric-based identity verification systems. E-Verify, for example, currently will require a screener to enter biographical data for its Internet-based database screening protocols, utilizing traditional enumeration systems (e.g., Social Security Number). However, E-Verify offers a "Photo Tool" and, thus, incorporates one type of biometric data technology: digital photo and digitalized photo databases. As will be discussed below in more detail in Part II, it appears that policymakers are now attempting to expand the E-Verify database screening protocol to utilize a universal biometric database. Specifically, it appears that Congress is recommending the implementation of a universal digitalized photo database of all citizens and noncitizens through the mandatory national expansion of E-Verify and E-Verify's Photo Tool, both of which are currently test pilot programs. This legislative proposal potentially suggests the future adoption of facial recognition technology for digitalized photo data matching. Finally, it is important to note that databases created to serve one kind of identity management system can be put to use for other identity management systems. Therefore, a universal digitalized photo database created for E-Verify, for instance, eventually could be used for S-COMM, FAST, and other database screening and identity determinations.

Table 2 compares the three types of identity management systems: identity verification, identity determination, and identity inference.

Table 2. Examples of Identity Management Systems[80]

	Identity Verification Systems	Identity Determination Systems	Identity Inference Systems
Description	Identity verification systems seek to confirm or authenticate identity data presented by an individual, checking produced data against an existing database.[81]	Identity determination systems seek to identify an individual's identity through processing either collected data (e.g., fingerprints provided) or captured data (e.g., facial recognition software from video) through existing databases.[82]	Identity inference systems seek to sort individuals through a process of "classification and exclusion" and "risk profiling" that can "result in different citizens being put in different risk categories based on the threat they are perceived to pose to the state."[83]
Primary Inquiry	"'Is this person who she says she is?'"[84]	"The system tries to answer the questions 'Who is this person?' or 'Who generated this biometric?'"[85]	How do you determine "'intent-based threat assessments of individuals and groups[?]'"[86]

80. Experts often refer to biometric data systems as "biometric recognition," "biometric identity verification," or "biometric identification" systems. Existing discourse does not use the terminology of "identity verification," "identity determination," or "identity inference" systems. My departure from the terminology is to emphasize that these three differing types of systems are all concerned with identity management as a policy prescription, and that not all systems are biometric-based. Yet, they each illustrate strands of government efforts, sometimes separate and sometimes in coordination, to place identity under surveillance, including under bureaucratized cybersurveillance. Many of the nonbiometric programs are either in the process of transforming into biometric ID cybersurveillance programs and/or are relying more upon digitalized biometric IDs and other digitalized ID devices.

81. LYNCH, *supra* note 3, at 5.

82. *Id.* For clarification, I refer to these systems as "identity determination" systems, whereas Lynch refers to these systems as "identification" systems. *Id.*

83. ROSEN, *supra* note 28, at 27; *see also* DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY 197 (1994); SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK, AND DIGITAL DISCRIMINATION 13 (David Lyon ed., 2003).

84. LYNCH, *supra* note 3, at 5.

85. *Id.*

86. Noah Shachtman, *Army Tracking Plan: Drones That Never Forget a Face*, WIRED.COM (Sept. 28, 2011, 6:30 AM), *available at* http://www.wired.com/dangerroom/2011/09/drones-never-forget-a-face/ (quoting Charles River Analytics).

Methodology	"Verification systems are generally described as a 1-to-1 matching system because the system tries to match the biometric [or other personally identifiable information] presented by the individual against a specific biometric [or other data] already on file."[87]	"[Determination systems] must check the biometric presented against all others already in the database. Described as a 1-to-*n* matching system, where *n* is the total number of biometrics in the database."[88]	"'[P]robablistic algorithms th[at] determine the likelihood of adversarial intent'"[89] or conduct other threat risk assessments, including simple aggregation of data. Identity inference systems may incorporate aspects of identity verification and identity determination systems.[90]
Examples	E-Verify, Systematic Alien Verification for Entitlements (SAVE), HAVA, Student and Exchange Visitor Information (SEVIS), United States Visitor and Immigrant Status Indicator Technology (US-VISIT)	S-COMM, FBI's Next Generation Identification (NGI), Use of facial recognition technology to identify individuals through mapping CCTV video surveillance footage and other video surveillance to digital photos uploaded on Facebook, Twitter, etc.[91]	FAST, Secure Flight ("No-Fly List"), Terrorist Watch List and Terrorist Identities Datamart Environment (TIDE) database, Automated Targeting System (ATS),[92] Adversary Behavior Acquisition, Collection, Understanding,

87. LYNCH, *supra* note 3, at 5.

88. *Id.*

89. Shachtman, *supra* note 86 (quoting Modus Operandi, Inc.).

90. *See id.*

91. *See infra* note 348.

92. *See, e.g.*, WILLIAM P. BLOSS, UNDER A WATCHFUL EYE: PRIVACY RIGHTS AND CRIMINAL JUSTICE 182 (2009).

> ATS was launched in the 1990s, automated in 2002, and originally designed to be a cargo screening tool for U.S. Customs and Border Protection to evaluate materials that may pose a threat to the nation. However, Homeland Security officials in 2006 modified the system to create a terrorist risk rating formula and perform screening of both inbound and outbound cargo, travelers, and conveyances. The model assigns a risk assessment score . . . . ATS maintains a voluminous database, and its risk profiles and scores will be kept for 40 years

			and Summarization (ABACUS),[93] Clear Heart,[94] Drone "Signature Strikes"[95]

unable to be inspected or reviewed. In spite of the past inaccuracies and flaws with counterterrorism threat profile regimes, this ambitious program to evaluate and catalog millions of people and pieces of merchandise illustrates the comprehensive goal of this generation of data gathering.

Id. (footnote omitted).

93. Shachtman, *supra* note 86.

94. *Id.*

95. Due to the covert nature of these operations, limited information is available on the exact nature of the cybersurveillance that may inform drone attacks and targeted killings in the "war on terror." *See generally* DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER 241–70 (2012) (describing use of drones and targeted killing strategy in the "war on terror"). Recently, more information has emerged on the use of "signature strikes": "a controversial [targeted killing] practice known as signature strikes, . . . or [targeting those with] defining characteristics associated with terrorist activity, but whose identities aren't necessarily known." DANIEL KLAIDMAN, KILL OR CAPTURE: THE WAR ON TERROR AND THE SOUL OF THE OBAMA PRESIDENCY 41 (2012). From media reports, it appears that signature strikes are informed in part by drone footage and potentially from other types of cybersurveillance. *See, e.g.*, Greg Miller, *Broader Drone Tactics Sought*, WASH. POST, Apr. 19, 2012, at A1, *available at* http://www.washingtonpost.com/world/national-security/cia-seeks-new-authority-to-expand-yemen-drone-campaign/2012/04/18/gIQAsaumRT_story.html ("The CIA is seeking authority to expand its covert drone campaign in Yemen by launching strikes against terrorism suspects even when it does not know the identities of those who could be killed, U.S. officials said. Securing permission to use these 'signature strikes' would allow the agency to hit targets based solely on intelligence indicating patterns of suspicious behavior, such as imagery showing militants gathering at known al-Qaeda compounds or unloading explosives."); Shachtman, *supra* note 86 (describing emerging cybersurveillance and biometric cybersurveillance technologies that could potentially assist in identity inference programs to identify potential terrorists through a "system [that] would integrate data from informants' tips, drone footage, and captured phone calls"); Lev Grossman, *Drone Home: They Fight for America Abroad, But What Happens When Drones Return Home?*, TIME, Feb.11, 2013, at 26, 30 ("According to reports in the New York Times and elsewhere, the Obama Administration conducts so-called signature strikes, which are aimed not at specific high-level targets but at any person or people whose behavior conforms to certain suspicious patterns."). "[T]he vast majority of drone attacks conducted by the United States have been signature strikes[.]" Kevin Jon Heller, *'One Hell of a Killing Machine': Signature Strikes and International Law*, 11 J. INT'L CRIM. JUST. 89, 89 (2013); *see also* Scott Shane, *Rights Groups, in Letter to Obama, Question Legality and Secrecy of Drone Killings*, N.Y. TIMES, Apr. 13, 2013, at A9, *available at* http://www.nytimes.com/2013/04/13/us/politics/rights-groups-question-legality-of-targeted-killing.html ("Ms. Schakowsky [Rep. Jan Schakowsky (D-Ill.)] was prompted to question Mr. Brennan [John O. Brennan, Director of CIA] in part by an article this week by McClatchy News Service reporting that it had obtained classified government documents showing that the drone strikes had killed hundreds of low-level suspected militants whose identities were not known."); Scott Shane, *Election Spurred a Move To Codify U.S. Drone Policy*, N.Y. TIMES, Nov. 25, 2012, at A1, *available at* http://www.nytimes.com/2012/11/25/world/white-house-presses-for-drone-rule-book.html ("[T]he word evolved to mean the

To help concretely frame each of type of identity program within the system, I will briefly describe three DHS identity management programs: E-Verify (identity verification), S-COMM (identity determination), and FAST (identity inference). Although E-Verify appears to be poised for mandatory national expansion through recently proposed immigration reform legislation, and S-COMM has already been mandated nationally as of 2013 through executive mandate, all three programs are based upon emerging, experimental, or speculative technologies. All three can be fairly characterized, therefore, as test pilot programs.

1. Identity Verification

"Under a[n identity] verification system, an individual presents herself as a specific person ('I am Jennifer'). The system checks her biometric (such as an iris scan) against the biometric already in the database linked to that person's file (Jennifer's iris print) to try to find a match."[96] For example, "[t]he E-Verify program . . . is a verification-based system."[97] The E-Verify program is currently a voluntary test pilot program.[98] Multiple state immigration laws, however, are now mandating that employers use E-Verify.[99] Under *Chamber of Commerce v. Whiting*, the Court upheld an Arizona statute, the Legal Arizona Workers Act, that requires all employers in the state of Arizona to conduct E-Verify Internet database screening on all new hires.[100]

'signature' or militants in general—for instance, young men toting arms in an area controlled by extremist groups. Such strikes have prompted the greatest conflict inside the Obama administration, with some officials questioning whether killing unidentified fighters is legally justified or worth the local backlash.").

96. LYNCH, *supra* note 3, at 5.

97. *Id.*

98. Chamber of Commerce v. Whiting, 131 S. Ct. 1968, 1975 (2011) ("Originally known as the 'Basic Pilot Program,' E–Verify 'is an internet-based system that allows an employer to verify an employee's work-authorization status.'" (quoting Chicanos Por La Causa, Inc. v. Napolitano, 558 F.3d 856, 862 (9th Cir. 2009))). Congress expressly prohibited DHS from requiring private employers to use E-Verify on anything other than a voluntary basis. *See* Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, § 402, 110 Stat. 3009-546, 3009-656 (codified at 8 U.S.C. § 1324a); *see also Whiting*, 131 S. Ct. at 1985 ("'[T]he Secretary of Homeland Security may not require any person or . . . entity [outside the Federal Government] to participate in a pilot program' such as E-Verify." (quoting the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 § 402(a))); Hu, *supra* note 13, at 579–99.

99. Hu, *supra* note 13, at 608–09 ("The state-by-state patchwork of E-Verify schemes is especially problematic, as several states require some or all employers use E-Verify. Alabama, Arizona, and Mississippi require all employers to use E-Verify. Georgia, Louisiana, North Carolina, South Carolina, Tennessee, and Utah require most employers to use E-Verify. . . . Many other states require subsets of employers—such as public employers, contractors, and subcontractors—to enroll in E-Verify. These states include Colorado, Florida, Idaho, Indiana, Michigan, Missouri, Nebraska, Oklahoma, Pennsylvania, Virginia, West Virginia." (footnotes omitted)).

100. *Whiting*, 131 S. Ct. at 1985 (holding that Arizona immigration statute requiring employers engage in mandatory E-Verify database screening is not preempted by federal immigration law because federal law only prohibits federal government from mandating

The E-Verify system is complex, relying upon statistical algorithms and multiple databases in order to conclude that the identity and citizenship status of an individual has been sufficiently "verified."[101] To oversimplify, however, one can say that E-Verify works in the following way. First, after an employer receives the E-Verify online software program from DHS, an employer collects personally identifiable data from an employee (e.g., name, date of birth, and Social Security Number).[102] Next, this information is entered by the employer or an employer's "designated agent" into a software program that is accessible online, free of cost.[103] The software runs the data first through the SSA database and then through DHS immigration databases.[104] The program informs the employer within seconds whether an individual is "confirmed" or "verified."[105] If there is an anomalous result in the database screening algorithms, however, the individual falls within a category titled "Tentative Nonconfirmation" (TNC).[106] Pursuant to the guidelines set forth by the program, an employer is then required to allow an employee to contest the TNC result.[107] An employee must contact DHS or SSA within eight business days to resolve the TNC result. If an employee is unable to resolve the

---

E-Verify, and nothing in the federal law prohibits states from mandating E-Verify). The Court concluded, "[t]he provision of IIRIRA setting up the program that includes E-Verify contains no language circumscribing state action. It does, however, constrain federal action[.]" *Id.*; *see also* Hu, *supra* note 13, at 598–99.

101. *See, e.g.*, WESTAT, WESTAT EVALUATION OF THE E-VERIFY PROGRAM: USCIS SYNOPSIS OF KEY FINDINGS AND PROGRAM IMPLICATIONS (2010), *available at* http://www.uscis.gov/USCIS/Native%20Docs/Westat%20Evaluation%20of%20the%20E-Verify%20Program.pdf; *E-Verify: Preserving Jobs for American Workers*, *Hearing Before the Subcomm. on Immigration Policy and Enforcement of the H. Comm. on the Judiciary*, 112th Cong. 34–35 (2011) (written testimony of Theresa C. Bertucci, Assoc. Dir., Enter. Servs. Directorate, U.S. Citizenship & Immigration Servs.).

102. U.S. CITIZENSHIP & IMMIGRATION SERVS., I AM AN EMPLOYER: HOW DO I . . . USE E-VERIFY? 1–2 (2008*)*, *available at* http://www.uscis.gov/USCIS/Resources/E4en.pdf.

103. *Id.*

104. The Social Security Administration maintains the Numerical Identification File (NUMIDENT) Social Security Number database, which includes the name, date of birth, and other biographical information of Social Security Administration applicants. ANDORRA BRUNO, CONG. RESEARCH SERV., R40446, ELECTRONIC EMPLOYMENT ELIGIBILITY VERIFICATION 2 (2009). United States Citizenship and Immigration Services maintains the Verification Information System (VIS) database, which is "comprised of citizenship, immigration, and employment status information from several DHS System of Records." U.S. CITIZENSHIP & IMMIGRATION SERVS., U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE VERIFICATION INFORMATION SYSTEM SUPPORTING VERIFICATION PROGRAMS 2 (2007), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_vis.pdf.

105. *The Verification Process*, U.S. CITIZENSHIP & IMMIGRATION SERVS. (May 7, 2012), http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=d4abfb41c8596210VgnVCM100000b92ca60aRCRD&vgnextchannel=d4abfb41c8596210VgnVCM100000b92ca60aRCRD.

106. *Id.*

107. *Employee Rights and Responsibilities*, U.S. CITIZENSHIP & IMMIGRATION SERVS. (Sept. 14, 2012), http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=7279fb41c8596210VgnVCM100000b92ca60aRCRD&vgnextchannel=7279fb41c8596210VgnVCM100000b92ca60aRCRD.

TNC within eight business days, the system generates a "Final Nonconfirmation" (FNC) result, and an employer can terminate the employee.[108]

While E-Verify does not involve an algorithmic biometric data matching component, E-Verify does offer a biometric-driven identification tool: the E-Verify Photo Tool. Some policymakers argue that the E-Verify identity verification program should be expanded to include a biometric data matching component (e.g., matching a digital photo, fingerprint, or iris scan to universal government database(s)).[109] A biometric E-Verify program would thus offer a policy parallel to the biometric identity determination component of Secure Communities (S-COMM).

2. Identity Determination

S-COMM is an immigration status check program that facilitates federal government fingerprint database matching through biometric data collection by local and state law enforcement.[110] S-COMM is described as an identity determination program.[111] Identity determination systems seek to identify an individual's identity through processing either collected data (e.g., fingerprints scanned) or captured data (e.g., facial recognition technology using digital photos captured over the Internet or from video) through existing databases.[112] Identity determination systems are different from identity verification systems in important ways. Identity determination systems can be distinguished from identity "verification systems because an [identity determination] system seeks to identify an unknown person (or unknown biometric)."[113] S-COMM can be fairly described as a mandatory, test pilot program.[114] As of 2013, all state and local law

---

108. *DHS TNCs*, U.S. CITIZENSHIP & IMMIGRATION SERVS. (Oct. 13, 2011), http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=420d479347ea6210VgnVCM100000b92ca60aRCRD&vgnextchannel=420d479347ea6210VgnVCM100000b92ca60aRCRD; *see also* DEP'T OF HOMELAND SEC., THE E-VERIFY PROGRAM FOR EMPLOYMENT VERIFICATION MEMORANDUM OF UNDERSTANDING art. II.C.10 (2009), *available at* http://www.uscis.gov/USCIS/E-Verify/Customer%20Support/Employer%20MOU%20(September%202009).pdf ("If the employee does not choose to contest a tentative nonconfirmation or a photo non-match or if a secondary verification is completed and a final nonconfirmation is issued, then the Employer can find the employee is not work authorized and terminate the employee's employment.").

109. *See, e.g.*, GOV'T ACCOUNTABILITY OFFICE, GAO-11-146, EMPLOYMENT VERIFICATION: FEDERAL AGENCIES HAVE TAKEN STEPS TO IMPROVE E-VERIFY, BUT SIGNIFICANT CHALLENGES REMAIN 3 (2010) [hereinafter GAO EMPLOYMENT VERIFICATION].

110. LYNCH, *supra* note 3, at 3, 9.

111. *See id.*

112. *Id.* at 5.

113. *Id.*

114. S-COMM began as a test pilot program in fourteen jurisdictions in October 2008. AARTI KOHLI, PETER L. MARKOWITZ & LISA CHAVEZ, CHIEF JUSTICE EARL WARREN INST. ON LAW & SOC. POLICY, SECURE COMMUNITIES BY THE NUMBERS: AN ANALYSIS OF DEMOGRAPHICS AND DUE PROCESS 1 (2011), *available at* http://www.law.berkeley.edu/files/Secure_Communities_by_the_Numbers.pdf. In 2010, before the efficacy of the program could be fully assessed, however, DHS determined that all state and local law enforcement

enforcement jurisdictions must participate in requisite biometric data collection and database screening protocols pursuant to DHS mandate.[115]

Multiple state immigration laws are now mandating the expansion of data collection and database screening as a part of state and local identity management policymaking.[116] In particular, some state immigration laws now require state and local law enforcement officials to engage in the biometric data screening protocols that are operative in S-COMM, but in a way that encompasses a broader population than those targeted by S-COMM.[117] Under *Arizona v. United States*, for instance, the Court upheld Section 2(B) of the highly controversial Arizona Senate Bill 1070 (SB 1070), also referred to in the media as the "racial profiling" law and the "show

---

agencies would be required to implement S-COMM by 2013. *See* Memorandum from Riah Ramlogan, Deputy Principal Legal Advisor, for Beth N. Gibson, Assistant Deputy Dir., U.S. Immigration & Customs Enforcement, on Secure Communities – Mandatory in 2013 (Oct. 2, 2010), *available at* http://images.politico.com/global/2012/01/icefoiaoptoutdocs.pdf; *see also* Julia Preston, *Resistance Widens to Obama Initiative on Criminal Immigrants*, N.Y. TIMES, Aug. 13, 2011, at A11, *available at* http://www.nytimes.com/2011/08/13/us/politics/13secure.html.

115. *See* Kirk Semple & Julia Preston, *Deal To Share Fingerprints Is Dropped, Not Program*, N.Y. TIMES, Aug. 6, 2011, at A11, *available at* http://www.nytimes.com/2011/08/06/us/06immig.html; *supra* note 114.

116. For example, Arizona Senate Bill 1070 (SB 1070) includes such a database screening provision, Section 2(B), in the Support Our Law Enforcement and Safe Neighborhoods Act, ch. 113, 2010 Ariz. Sess. Laws 450 (codified in scattered sections of ARIZ. REV. STAT. ANN. §§ 11, 13, 23, 28, 41 (2010)), *amended by* Act of Apr. 30, 2010, ch. 211, 2010 Ariz. Sess. Laws 1070. Specifically, Section 2(B) is codified in ARIZ. REV. STAT. ANN. § 11-1051(B) (2012). For an overview of Section 2(B), see Hu, *supra* note 13, at 596–604.

117. Section 2(B) of SB 1070, for instance, uses the same database screening protocol as S-COMM pursuant to 8 U.S.C. § 1373(c) and mandates this database screening protocol through express incorporation of the federal immigration statute into the language of the state immigration statute.

> Section 2(B) of S.B. 1070 provides that, when Arizona law enforcement officers reasonably suspect that a person they have lawfully stopped, detained, or arrested is unlawfully present, "a reasonable attempt shall be made, when practicable, to determine the immigration status of the person" pursuant to the verification procedure established by Congress in 8 U.S.C. § 1373(c).

Arizona v. United States, 132 S. Ct. 2492, 2522 (2012) (Thomas, J., concurring in part and dissenting in part) (citing ARIZ. REV. STAT. ANN. § 11-1051(B) (2012)). Specifically, 8 U.S.C. § 1373(c) of the Immigration and Nationality Act (INA) allows the state to conduct an immigration status check and seek database-driven information from DHS to determine whether an individual is lawfully present in the United States.

> Pursuant to 8 U.S.C. § 1373(c), DHS is required to "respond to an inquiry by a Federal, State, or local government agency, seeking to verify or ascertain the citizenship or immigration status . . . for any purpose authorized by law, by providing the requested verification or status information." DHS has, in its discretion, set up LESC [Law Enforcement Support Center], which is administered by ICE and "serves as a national enforcement operations center that promptly provides immigration status and identity information to local, state, and federal law enforcement agencies regarding aliens suspected of, arrested for, or convicted of criminal activity."

United States v. Arizona, 703 F. Supp. 2d 980, 995 (D. Ariz. 2010).

me your papers" law.[118] Section 2(B) requires Arizona law enforcement officials to engage in mandatory biometric data collection and database screening of those suspected of unlawful presence, following the same screening protocols as S-COMM.[119] In contrast, S-COMM targets only arrestees.

S-COMM, as an identity determination system, requires local and state law enforcement agencies to run biometric and biographical data of arrestees through federal government databases to determine an individual's identity. Although a gross simplification, S-COMM works in the following way. After an arrest, a local law enforcement agency (LEA) scans and submits the fingerprints of an arrestee to be checked against FBI and DHS databases.[120] If there is a fingerprint match, the FBI sends an Immigration Alien Query (IAQ) to the Law Enforcement Support Center (LESC) that is managed by DHS's U.S. Immigration and Customs

---

118. *Arizona*, 132 S. Ct. at 2507–10 (holding that it was improper to enjoin Section 2(B) on preemption grounds because "if § 2(B) only requires state officers to conduct a status check during the course of an authorized, lawful detention or after a detainee has been released, the provision likely would survive preemption—at least absent some showing that it has other consequences that are adverse to federal law and its objectives").

119. *See* Hu, *supra* note 13, at 594 ("In Section 2(B) of SB 1070, Arizona mandates that local law enforcement determine—during the course of any lawful stop, arrest, or detention—whether an individual is lawfully present in the U.S., if the officer has reasonable cause to believe the individual may be unlawfully present. Section 2(B), as upheld in *Arizona*, first requires an inspection of physical documents (e.g., driver's license or immigration document). A follow-up database screening is mandated under Section 2(B) if an inspection of the physical identity document cannot confirm an individual's identity and citizenship status.").

120. The FBI maintains the IAFIS (Integrated Automated Fingerprint Identification System) database. *Integrated Automated Fingerprint Identification System*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis. DHS maintains the IDENT (Automated Biometric Identification System) database. "IDENT is a Department of Homeland Security (DHS)-wide system for the collection and processing of biometric and limited biographic information for DHS . . . ." U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT) 2 (2006) [hereinafter IDENT PRIVACY IMPACT ASSESSMENT], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf. The database screening process can be summarized as follows: "1. . . . [T]he arresting LEA [law enforcement agency] sends the subject's fingerprints and associated biographical information to CJIS [Criminal Justice Information Services]/IAFIS . . . . 2. CJIS electronically routes the subject's biometric and biographic information for all criminal answer required (CAR) transactions to US-VISIT/IDENT to determine if there is a fingerprint match with records in that system." U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, U.S. DEP'T OF HOMELAND SEC., SECURE COMMUNITIES: QUARTERLY REPORT: FISCAL YEAR 2010 REPORT TO CONGRESS FOURTH QUARTER 2–3 (2011), *available at* http://www.ice.gov/doclib/foia/secure_communities/congressionalstatusreportfy104thquarter.pdf.

Enforcement (ICE).[121] The LESC staff research multiple databases to determine whether someone should be subject to detention and deportation.[122]

3. Identity Inference

An identity inference program allows for the government and its delegates to infer threat risk, for instance potential criminality or terroristic threat risk. The Future Attribute Screening Technology (FAST) is an example of an identity inference program.[123] FAST is currently under testing by DHS and has been described in press reports as a "precrime" program.[124] If implemented, FAST will purportedly rely upon complex statistical algorithms that can aggregate data from multiple databases in an attempt to "predict" future criminal or terrorist acts, most likely through stealth cybersurveillance and covert data monitoring of ordinary citizens.[125] The FAST program purports to assess whether an individual might pose a "precrime" threat through the capture of a range of data, including biometric data.[126] In other words, FAST attempts to infer the security threat risk of future criminals and terrorists through data analysis.

Under FAST, biometric-based physiological and behavioral cues are captured through the following types of biometric data: body and eye movements, eye blink rate and pupil variation, body heat changes, and breathing patterns.[127] Biometric-based linguistic cues include the capture of the following types of biometric data: voice pitch changes, alterations in rhythm, and changes in intonations of speech.[128] Documents released by DHS indicate that individuals could be arrested and face other serious consequences based upon statistical algorithms and predictive analytical assessments.[129] Specifically, projected consequences of FAST "can range from none to being temporarily detained to deportation, prison, or death."[130]

---

121. U.S. DEP'T OF HOMELAND SEC., IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE) SECURE COMMUNITIES (SC) STANDARD OPERATING PROCEDURES (SOP) 4 (2009), *available at* http://epic.org/privacy/secure_communities/securecommunitiesops93009.pdf.

122. *Id.* at 4–5.

123. *See* Privacy Impact Assessment for FAST (2008), *supra* note 74.

124. *See Future Attribute Screening Technology (FAST) Project FOIA Request*, EPIC, http://epic.org/privacy/fastproject/; Declan McCullagh, *Homeland Security Moves Forward with 'Pre-Crime' Detection*, CNET NEWS (Oct. 7, 2011, 4:00 AM), http://news.cnet.com/8301-31921_3-20117058-281/homeland-security-moves-forward-with-pre-crime-detection/.

125. *See* McCullagh, *supra* note 124; U.S. Dep't of Homeland Sec., Presentation: Future Attribute Screening Technology (July 28, 2010), *available at* http://epic.org/privacy/fastpresentation.pdf.

126. *See* McCullagh, *supra* note 124.

127. Privacy Impact Assessment for FAST (2008), *supra* note 74, at 4; *Future Attribute Screening Technology (FAST) Project FOIA Request*, *supra* note 124; U.S. Dep't of Homeland Sec., *supra* note 125.

128. Privacy Impact Assessment for FAST (2008), *supra* note 74, at 4; McCullagh, *supra* note 124; U.S. Dep't of Homeland Sec., *supra* note 125.

129. Privacy Impact Assessment for FAST (2008), *supra* note 74, at 2.

130. *Id.*

C. Cybersurveillance and Dataveillance Capacities of Digitalized Biometric IDs

Identity management systems encourage the expansion of digitalized ID trackers that can serve as unique identifiers or data signatures. This allows for the more efficient identification of individuals during in-person encounters or through virtual encounters. These encounters allow the government or its delegates to conduct database screening and then take action, for example, based upon data matches[131] or data mismatches[132] which are considered suspicious. The discussion below explains how digitalized biometric IDs can serve not only as a traditional form of identity registration (e.g., providing biographical data through driver's license application and passport application), but now also may serve a variety of tracking functions under emerging technologies, including geolocational, biometric, behavioral, and biographical tracking.

1. Digitalized Biometric IDs: Geolocational Tracking

To understand the emerging tracking capacities of IDs that can be embedded with radio frequency identification (RFID)—such as passports, driver's licenses, and "high-tech" Social Security Cards—a brief introduction to RFID technology is necessary. The advent of RFID technology has added a geolocational surveillance angle to modern identification credentialing programs.[133] RFID allows for the monitoring of an individual's movement through hand-held devices as well as other

---

131. Data matches trigger heightened suspicion in data and database screenings pursuant to S-COMM and the No-Fly List. *See, e.g.*, *Secure Communities*, U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, http://www.ice.gov/secure_communities/ (explaining that if a match is detected through the screening process, "ICE then reviews other databases to determine whether the person is here illegally or is otherwise removable"); *"False Match" Shows No-Fly List Isn't Perfect*, CBS NEWS (May 6, 2010, 2:58 PM), http://www.cbsnews.com/2100-201_162-6466411.html.

132. Data mismatches trigger heightened suspicion under the database screening protocols in E-Verify and HAVA. *See, e.g.*, *Statement for the Record: E-Verify*, U.S. CITIZENSHIP & IMMIGRATION SERVS. (May 20, 2008), http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=bca6fa693660a110VgnVCM10000004718190aRCRD ("In almost every case, a mismatch will occur either because the employee is actually not authorized to work . . . ; because the employee has not yet updated his or her records with SSA . . . ; or because the employer made an error inputting information into the system."); *see also Senate Bill Implementing Help America Vote Act (HAVA) Would Disenfranchise Thousands of New Yorkers*, BRENNAN CTR. FOR JUSTICE AT N.Y. UNIV. SCH. OF LAW (Mar. 21, 2005), http://www.brennancenter.org/press-release/senate-bill-implementing-help-america-vote-act-hava-would-disenfranchise-thousands-new (describing how Social Security Number mismatches under HAVA database screening can disenfranchise voters).

133. *See* BILL GLOVER & HIMANSHU BHATT, RFID ESSENTIALS 30–31, 55 (2006). RFID tags can either be passive or active. *Id.* at 58. Active tags are powered internally, while passive tags are briefly activated by the radio frequency scan of the reader. *Id. See* Alírio J. Soares Boaventura & Nuno Borges Carvalho, *Extending Reading Range of Commercial RFID Readers*, 61 IEEE TRANSACTIONS ON MICROWAVE THEORY & TECHS. 633 (2013), *available at* http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6376259.

tracking devices. That technology renders GPS surveillance moot in some circumstances, or allows for the augmentation of GPS-like geolocational tracking in other circumstances,[134] because it enables the insertion of what is in effect a personal tracking device into identity cards that people may carry out of necessity or by requirement of the law (e.g., a driver's license).

ID documents such as driver's licenses in some states and all U.S. passports are now implanted with RFID technology. Since 2007, each U.S. passport is now implanted with an RFID chip in the booklet's back cover.[135] Additionally, the REAL ID Act of 2005 requires the inclusion of "common machine-readable technology" in all REAL ID-compliant driver's licenses.[136] Several states now issue RFID "enhanced driver's licenses," including Michigan, New York, Vermont, and Washington.[137]

Emergency response personnel in some jurisdictions now carry enhanced identification cards that are outfitted with RFID technology in order to facilitate the location and identification of personnel in emergency situations.[138] The human implantation of RFID microchips is now FDA approved.[139] New RFID technology

---

134. *See, e.g.*, *Ennovasys Announces Its RFID-GPS Integrated Solution To Improve the Safety of School Children – TrakSchool™*, PRWEB (Aug. 15, 2011), http://www.prweb.com/releases/2011/8/prweb8712635.htm (TrakSchool technology allows parents and school authorities to monitor the whereabouts of children using a GPS-RFID device and proprietary software that allows for the visualization of this data).

135. U.S. passports contain RFID chips "encoded with the bearer's personal information printed on the data page, a digitized version of the bearer's photograph, a unique chip number, and a digital signature to protect the integrity of the stored information." 22 C.F.R. § 51.1(b) (2012).

136. REAL ID Act of 2005, Pub. L. No. 109-13, § 202(a)(1), (b)(8)–(9), 119 Stat. 302, 312. Although the REAL ID Act does not require the inclusion of RFID technology in REAL ID-compliant driver's licenses, it appears that Congress has authorized the DHS Secretary to impose such a requirement through administrative rulemaking. *Id.* § 205(a), 119 Stat. at 315 ("All authority to issue regulations, set standards, and issue grants under this title shall be carried out by the [DHS] Secretary, in consultation with the Secretary of Transportation and the States."); *see also* Anita Ramasastry, *Why the 'Real ID' Act Is a Real Mess*, CNN.COM (Aug. 12, 2005, 2:36 PM), http://www.cnn.com/2005/LAW/08/12/ramasastry.ids/index.html ("In the past, the Department of Homeland Security has indicated it likes the concept of RFID chips.").

137. *Enhanced Drivers Licenses: What Are They?*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/enhanced-drivers-licenses-what-are-they.

138. *See* Tiffany Fox, *Go-Anywhere Tracking of First Responders with WIISARD Radio-Frequency System*, PHYS.ORG (Nov. 11, 2010), http://phys.org/news/2010-11-go-anywhere-tracking-wiisard-radio-frequency.html; *New First Response RFID System Developed*, HOMELAND SEC. NEWS WIRE (Sept. 8, 2008), http://www.homelandsecuritynewswire.com/new-first-response-rfid-system-developed.

139. VeriChip Corporation received FDA approval for human implantation of the VeriChip RFID microchip in 2004. Todd Lewan, *Chip Implants Linked to Animal Tumors*, WASH. POST (Sept. 8, 2007, 2:04 PM), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/09/08/AR2007090800997_pf.html (explaining chip implant was approved by FDA in December 2004 despite tests that indicated that the technology was unsafe) ("The FDA is overseen by the Department of Health and Human Services, which, at the time of VeriChip's approval, was headed by Tommy Thompson. Two weeks after the

is being tested on human volunteers who are willing to be "chipped" through surgical implantation of the microchip in the body.[140]

According to reports, the RFID tracking device embedded in U.S. passports can be read from a distance of around 20 feet.[141] In response to criticism that data on U.S. passports could be maliciously or inadvertently stolen, the U.S. Department of State upgraded the protection of the RFID-enhanced U.S. passports to incorporate a thin metal lining to make it more difficult for unauthorized readers to "skim" or "steal" the information encoded on the RFID chip.[142] Reports describing security measures taken to protect the information encoded on the RFID chip have explained that the State Department has adopted a Basic Access Control (BAC) system, which apparently functions as a Personal Identification Number (PIN) that must be entered into an RFID reader before the chip can be read.[143] The BAC purports to encrypt all communications between the RFID chip and the "interrogator" of the chip information.[144]

The RFID passports are interoperable with the systems of other nations, complying with the standards and technological specifications developed by the International Civil Aviation Organization (ICAO).[145] The ICAO requires a minimum capacity of thirty-two kilobytes of memory for storage on the passport RFID chip.[146] However, the U.S. Department of State has included a chip that has sixty-four kilobytes of memory, double the minimum required data storage capacity.[147] The State Department has explained that the purpose for this extra storage is to allow for the implantation of additional biometric data,[148] such as fingerprints, iris scans, and potentially DNA. According to press reports, "[b]efore the department adds additional data or biometric identifier other than a digitized

---

device's approval took effect on Jan. 10, 2005, Thompson left his Cabinet post, and within five months was a board member of VeriChip Corp. and Applied Digital Solutions. He was compensated in cash and stock options.").

140. *See* David Streitfeld, *First Humans To Receive ID Chips; Technology: Device Injected Under the Skin Will Provide Identification and Medical Information*, L.A. TIMES, May 9, 2002.

141. Chris Corum, *Contactless Inlays from SMARTRAC Ordered for US ePassport Project*, SECUREIDNEWS (Nov. 30, 2006), http:// secureidnews.com/news-item/contactless-inlays-from-smartrac-ordered-for-us-epassport-project/; Tom Corelis, *U.S. State Department Approves RFID Passports Amidst Privacy Concerns*, DAILYTECH (Jan. 4, 2008, 9:45 AM), http://www.dailytech.com/US+State+Department+Approves+RFID+Passports+Amidst+Privacy+Concerns/article10200.htm (pointing out that the new passports are "[r]eadable at up to 20 feet").

142. *Summary of Baird RFID Monthly for August*, RFID JOURNAL (Aug. 21, 2006), http://www.rfidjournal.com/articles/view?6562 (explaining that RFID "passports will incorporate a thin metal lining to prevent unauthorized readers from 'skimming' information when the passport is closed").

143. Electronic Passport, 70 Fed. Reg. 61,553, 61,554 (Oct. 25, 2005) (to be codified at 22 C.F.R. pt. 51).

144. *Id.*

145. *Id.* at 61,553.

146. *Id.*

147. Paul Prince, *United States Sets Date for E-Passports*, RFIDJOURNAL.COM (Oct. 25, 2005), http://www.rfidjournal.com/article/articleview/1951/1/132/.

148. *See id.*

photograph, however, it says it will seek public comment through a new rule-making process."[149]

It is also important to place RFID tracking within this context: RFID and GPS satellite tracking technologies are merging.[150] Therefore, ID documents have the potential to serve comprehensive 24/7 geolocational surveillance purposes. This requires a radical rethinking of Fourth Amendment jurisprudence because ID surveillance tracking of the body and biography can be conducted comprehensively, virtually, and near invisibly. Thus, ID documents implanted with GPS-RFID technology may likely provide the government with the capacity to conduct continuous or near-continuous geospatial monitoring, as well as biographical tracking, through such IDs.[151]

2. Digitalized Biometric IDs: Biometric Tracking

In the years after September 11, 2001, President George W. Bush signed several dozen executive orders entitled "Homeland Security Presidential Directives" (HSPDs) or "National Security Presidential Directives" (NSPDs).[152] Among these, HSPD-12 is the most relevant to this Article. HSPD-12 created a digitalized biometric ID credentialing requirement for federal government workers and

---

149. *Id.*

150. RFID and GPS technologies are merging in that more and more devices appear to incorporate both RFID tracking and GPS tracking capacities in a single device. *See* Manon G. Guillemette, Isabelle Fontaine & Claude Caron, *Hybrid RFID-GPS Real-Time Location System for Human Resources: Development, Impacts and Perspectives, Proceedings of the 41st Annual Hawaii International Conference on System Sciences* (2008); David H. Williams & Gary Hartwig, *How Will the Convergence of Location Technologies Such as RFID, GPS, RTLS, and LBS Affect Business?*, NBIZ MAG., Summer 2008, at 23, *available at* http://www.nbizmag.com/magarticles/rfid.pdf; *CS101 Handheld RFID Reader Adds GPS & Cellular Communication*, RFID.NET (Feb. 8, 2012), http://rfid.net/product-listing/reviews/176-csl-cs101-handheld-reader; *see also* Beth Bacheldor, *Hybrid Tag Includes Active RFID, GPS, Satellite and Sensors*, RFIDJOURNAL.COM (Feb. 24, 2009), http://www.rfidjournal.com/article/view/4635.

151. Ironically, however, experts also note that those who fall outside of the law will not possess such documents and will not be subject to this cybersurveillance. *See* HARPER, *supra* note 8, at 209 (explaining that terrorists have traditionally used legitimate documents) ("As we have seen, terrorists in the United States have made spare use of false identification or anonymity and, when they have, it has minimized their effectiveness.").

152. In addition to HSPD-12, President Bush signed at least three additional HSPDs that relate to biometric screening technology either implicitly or explicitly: HSPD-6, HSPD-11, and HSPD-24. *See* Homeland Security Presidential Directive/HSPD-6—Integration and Use of Screening Information To Protect Against Terrorism, 2 PUB. PAPERS 1174–75 (Sept. 16, 2003), *available at* http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf; Homeland Security Presidential Directive/HSPD-11—Directive on Comprehensive Terrorist-Related Screening Procedures, 2 PUB. PAPERS 1763–65 (Aug. 27, 2004), *available at* http://www.gpo.gov/fdsys/pkg/PPP-2004-book2/pdf/PPP-2004-book2-doc-pg1763.pdf; Homeland Security Presidential Directive/HSPD-24—Directive on Biometrics for Identification and Screening To Enhance National Security, 44 WEEKLY COMP. PRES. DOC. 788 (June 5, 2008), *available at* http://www.gpo.gov/fdsys/pkg/WCPD-2008-06-09/pdf/WCPD-2008-06-09-Pg788-2.pdf.

contractors. Specifically, HSPD-12, entitled Policy for a Common Identification Standard for Federal Employees and Contractors, required the establishment of a government-wide minimum standard for the issuance of a secure identification card or uniform identification credential to all federal employees and all government contractors.[153] HSPD-12, however, did not specify how to achieve that goal. The U.S. Department of Commerce and the National Institute of Standards and Technology (NIST) subsequently concluded HSPD-12 required the development and issuance of a personal identity verification (PIV) digitalized ID card containing biometric and other personal data.[154] The PIV card is machine readable and records points of entry and exit by federal employees and contractors.[155] The PIV card provides an example of a digitalized biometric ID card that has already been fully implemented.

The PIV card required by HSPD-12 is known in the identity management industry as a "smart card." The Smart Card Alliance is a coalition of industry partners that promote public and private sector use of smart cards for a variety of purposes.[156] The Alliance defines a smart card in this way:

> A smart card is a device that includes an embedded integrated circuit chip (ICC) that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of

---

153. Homeland Security Presidential Directive/HSPD-12—Policy for a Common Identification Standard for Federal Employees and Contractors, 2 PUB. PAPERS 1765–67 (Aug. 27, 2004) [hereinafter HSPD-12], *available at* http://www.gpo.gov/fdsys/pkg/PPP-2004-book2/pdf/PPP-2004-book2-doc-pg1765.pdf.

154. *About Personal Identity Verification (PIV) of Federal Employees and Contractors*, COMPUTER SEC. RES. CTR., http://csrc.nist.gov/groups/SNS/piv/index.html .

155. Memorandum from Karen S. Evans, Adm'r, Office of E-Government & Info. Tech., for the Chief Information Officers on Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12, at 9 (Feb. 17, 2006), *available at* http://159.142.166.204/Documents/Sample_Privacy_Documents_for_HSPD-12.pdf. Each federal agency was directed to develop a background check and credentialing program pursuant to HSPD-12 prior to issuing the PIV card to federal employees and contractors. Memorandum from Joshua B. Bolten, Dir., Office of Mgmt. and Budget, for the Heads of All Departments and Agencies on Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors (Aug. 5, 2005) [hereinafter 2005 OMB Memorandum], *available at* http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.

156. *About the Alliance: Overview*, SMART CARD ALLIANCE, http://www.smartcardalliance.org/pages/alliance.

> form factors, including plastic cards, fobs, subscriber identity modules (SIMs) used in GSM mobile phones, and USB-based tokens.[157]

In the case of the government PIV card, the smart card is an employee-carried ID that contains biometric data. The card is machine readable, and the employee brings the card into contact with a machine at workplace checkpoints to gain entrance.[158] The HSPD-12 PIV card, however, is not the only biometric ID card that is currently being implemented by the federal government and state governments.

Table 3 provides examples of credentialing programs that require the collection of digitalized biometric data to support the ID card. Programs such as HSPD-12's PIV card (scanned fingerprints and digital photograph), and REAL ID driver's licenses and e-Passports (digital photograph), are particularly important because they may serve as prototypes for future digitalized biometric ID credentialing systems ("high-tech" Social Security Cards or biometric E-Verify system).

Table 3. Examples of Biometric ID Credentialing Programs

Program	Entity	Description
Personal Identification Verification (PIV) card, or digitalized biometric ID required under Homeland Security Presidential Directive 12 (HSPD-12)[159]	Department of Commerce/National Institute of Standards and Technology (NIST)/Office of Personnel Management (OPM)[160]	Biometric ID credentialing program and background check for all federal workers and federal contractors under private employers. Biometric data collected: fingerprints and digital photographs.[161]
Transportation Worker Identification Credential (TWIC)[162]	Transportation Security Administration (TSA) /U.S. Coast Guard	Biometric ID credentialing program for the maritime transportation system. Biometric data collected: fingerprints and digital photographs.[163]

157. *Smart Card Primer*, SMART CARD ALLIANCE, http://www.smartcardalliance.org/pages/smart-cards-intro-primer.

158. *See* NAT'L INST. OF STANDARDS & TECH., PERSONAL IDENTITY VERIFICATION (PIV) OF FEDERAL EMPLOYEES AND CONTRACTORS 50 (2006), *available at* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

159. HSPD-12, *supra* note 153.

160. All federal agencies are required to implement HSPD-12. *See* 2005 OMB Memorandum, supra note 155.

161. *See* HSPD-12, *supra* note 153.

162. Established through the Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, § 102, 116 Stat. 2064, 2073 (codified as amended at 46 U.S.C. § 70105).

163. *Program Information*, TRANSP. SEC. ADMIN., http:// http://www.tsa.gov/

Border Crossing Card (BCC)[164]	DHS	Biometric ID credentialing program to facilitate border crossing between U.S. and Mexico border.[165] Biometric data collected: fingerprints and digital photographs.[166]
Employment Authorization Document (EAD)	U.S. Citizenship and Immigration Services (USCIS)	Biometric ID credentialing program for lawful immigrants (e.g., Temporary Protected Status immigrants). Biometric data collected: fingerprints and digital photographs.[167]
Lawful Permanent Resident Card (Green Card)	USCIS	Biometric data collected: fingerprints and digital photographs.[168]
U.S. Passport and e-Passport	U.S. Department of State (DoS)	Biometric data collected: digital photographs.[169]
REAL ID Driver's License[170]	TSA	Biometric data collected: digital photographs.[171]
Identity Management System (IDMS)	DoS	Biometric ID credentialing program for those requiring DoS ID cards. Biometric data

stakeholders/program-information.

164. The legal basis for the issuance of Border Crossing cards is the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, § 104, 110 Stat. 3009-546, 3009-555 to 3009-556 (codified as amended at 8 U.S.C. § 1101(a)(6)).

165. *See* U.S. DEP'T OF STATE, *Border Crossing Card*, TRAVEL.STATE.GOV, http://travel.state.gov/visa/temp/types/types_1266.html.

166. Jennifer 8. Lee, *Progress Seen in Border Tests of ID System*, N.Y. TIMES, Feb. 7, 2003, at 14, *available at* http://www.nytimes.com/2003/02/07/politics/07IMMI.html ("ID cards [are] encrypted with digital photos, signatures, biographical information and fingerprints . . . .").

167. *See* Dawn M. Lurie & Lindsey Baldwin, *USCIS' Fraud Detection Efforts Continue: Employment Authorization Document and Permanent Residence Card Redesigned*, GREENBERGTRAURIG (June 2010), http://www2.gtlaw.com/practices/immigration/compliance/pdf/GTAlert_USCIS_Fraud_June2010.pdf.

168. *See* News Release, U.S. Citizenship & Immigration Servs., USCIS to Issue Redesigned Green Card (May 11, 2010), *available at* http://www.aila.org/content/default.aspx?docid=31962.

169. *See* U.S. DEP'T OF STATE, *Digital Image Requirements*, TRAVEL.STATE.GOV, http://travel.state.gov/visa/visaphotoreq/digitalimagereq/digitalimagereq_5327.html.

170. As required under the REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 302 (codified as amended in scattered sections of 8 U.S.C.).

171. *Id.* § 202(b)(5), 119 Stat. at 312; *see also* 6 C.F.R. § 37.17(e) (2012).

		collected: fingerprints and digital photographs.[172]

3. Digitalized Biometric IDs: Biographical Tracking

Besides accumulating data regarding geolocational movements and serving as a vehicle for biometric data collection, digitalized biometric IDs are increasingly able to harvest general behavioral and biographical data that can help piece together a picture of the sum of personal habits and activities. "Smart card" technology now allows for the integration and aggregation of data across public and private systems.[173] The incorporation of smart card technology into products (e.g., credit and debit cards) and IDs allows for a more seamless integration of mass dataveillance capacity by both the federal government and the private sector.

A proliferation of smart card technology has increased the use of such digital ID technology to restrict not only physical access but "logical access" as well.[174] "Logical access" restriction can limit one's ability to access computer and Internet services, telecommunication devices, vehicles, ATM machines, and other products that can be keyed to a smart card as a matter of security.[175] Therefore, the interoperability of smart cards across multiple private and public sector platforms increases the capacity of both cybersurveillance and dataveillance. Logical access restriction further allows both the public and private sectors to more accurately pinpoint personally identifiable data and to develop profiles of individuals' histories and records of activities.

Table 4 shows that public and private entities can increasingly rely upon smart cards to restrict logical access as well as physical access.

---

172. *See* U.S. DEP'T OF STATE, PRIVACY IMPACT ASSESSMENT: IDENTITY MANAGEMENT SYSTEM (IDMS) (2009), *available at* http://www.state.gov/documents/organization/122507.pdf; STATE–72 Identity Management System (IDMS), 71 Fed. Reg. 62,653 (Oct. 26, 2006).

173. Integration and aggregation of data is made possible by technological interoperability and the development of compatible public and private systems. *See, e.g.*, SMART CARD ALLIANCE, PRIVACY AND SECURE IDENTIFICATION SYSTEMS: THE ROLE OF SMART CARDS AS A PRIVACY-ENABLING TECHNOLOGY 24 (2003), *available at* http://www.smartcardalliance.org/resources/lib/Privacy_White_Paper.pdf ("The Health Passport Project (HPP) is an initiative sponsored by the Western Governors' Association (WGA), with pilot implementation conducted in Bismarck, North Dakota, Cheyenne, Wyoming, and Reno, Nevada. The project was originally designed to provide a secure, versatile, multi-purpose electronic card to streamline access to and delivery of a variety of public and private services and benefits.").

174. *See infra* Table 4.

175. For further discussion of logical access controls, see, for example, Jeff Nigriny, *Integrating Physical and Logical Access Control*, ENTER. SYS. (Mar. 22, 2011), http://esj.com/Articles/2011/03/22/Integrating-Access-Control.aspx; *Logical Access Control Biometrics*, FINDBIOMETRICS, http://findbiometrics.com/applications/logical-access-control/.

Table 4. Examples of ID Cards and Logical Access Restriction

Program	Entity/Country	Description
PIV card swiped for computer access	DOJ	Smart card keyboards require PIV card for logical access to computer.[176]
HP Smart Card Keyboard	HP	Used to prevent unauthorized access to computers and networks; compatible with the DoD Common Access Card (CAC).[177]
ID card required to access the Internet	China	Citizens present ID cards when contracting for Internet access and publishing information online.[178]

This logical access restriction, if implemented on a national scale, would likely require ID verification before an individual is allowed to access certain information technologies. It would, of course, also create a record of an individual's use of those same technologies. Given that smart cards are achieving widespread use internationally, therefore, they may serve as a potential prototype for a digitalized biometric national ID.

Table 5 demonstrates that the federal government is increasingly integrating smart card technology into government-issued ID cards, including U.S. passports.

Table 5. Examples of Federal "Smart Card" Systems

Entity	"Smart Card"
Office of Personnel Management (OPM)	HSPD-12 PIV (Personal Identity Verification) Card[179]
U.S. Department of Defense (DoD)	Common Access Card[180]

176. DEP'T OF JUSTICE, PRIVACY IMPACT ASSESSMENT FOR THE PERSONAL IDENTITY VERIFICATION (PIV) CARD SYSTEM (2011), *available at* http://www.justice.gov/opcl/docs/pia-pivcard-hspd12.pdf.

177. *See Quick Specs: HP USB Smart Card Keyboard*, HEWLETT-PACKARD, http://h18000.www1.hp.com/products/quickspecs/archives_Canada/12346_ca_v4/12346_ca.pdf.

178. *China Considers Requiring Real Names, Government ID Cards, To Sign Up for Internet Access*, N.Y. DAILY NEWS (Dec. 26, 2012, 9:08 AM), http://www.nydailynews.com/news/world/china-require-real-internet-access-article-1.1227414; *China To Require ID for Internet Access*, LAPRENSASA.COM (Dec. 28, 2012), http://www.laprensasa.com/309_america-in-english/1873222_china-to-require-id-for-internet-access.html.

179. HSPD-12, *supra* note 153.

180. *Common Access Card (CAC)*, DOD ID CARD REFERENCE CTR., http://www.cac.mil/common-access-card/.

TSA/U.S. Coast Guard	TWIC (Transportation Workers Identification Credential) Card[181]
Federal Emergency Management Authority (FEMA)	FRAC (First Responder Authentication Credential) [182]
DoS	e-Passport[183]

II. PROPOSALS FOR A BIOMETRIC NATIONAL ID SYSTEM

Multiple policy proposals since 9/11 have contemplated the national adoption of a digitalized biometric ID system.[184] The growing prevalence of a universal biometric data collection mandate is now reflected in recent comprehensive immigration reform proposals, including the 2013 Bipartisan Senate Comprehensive Immigration Reform Bill.

A. Comprehensive Immigration Reform Proposals

In two recent comprehensive immigration reform proposals[185] introduced by a slate of bipartisan Senators on January 28, 2013,[186] and by President Obama on

---

181. *Program Information*, *supra* note 163.

182. *First Responder Authentication Credentials*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/first-responder-authentication-credentials.

183. *The U.S. Electronic Passport*, TRAVEL.STATE.GOV, http://travel.state.gov/passport/passport_2498.html.

184. For example, the Real Enforcement with Practical Answers for Immigration Reform (REPAIR) Proposal was released on April 29, 2010, by the Offices of Senators Reid (D-NV), Schumer (D-NY), Menendez (D-NJ), Leahy (D-VT), Durbin (D-IL), and Feinstein (D-CA). DICK DURBIN, DIANNE FEINSTEIN, PATRICK LEAHY, BOB MENENDEZ, HARRY REID & CHUCK SCHUMER, REAL ENFORCEMENT WITH PRACTICAL ANSWERS FOR IMMIGRATION REFORM (REPAIR) PROPOSAL (2010) [hereinafter REPAIR], *available at* http://thehill.com/images/stories/news/2010/PDFs/immigration2.pdf. Ten pages of the 26-page-long proposal discuss the use of a biometric employment verification system in a section entitled, Ending Illegal Employment through Biometric Employment Verification. Proponents of the immigration reform plan claimed that the Biometric Employment Verification system would utilize a "high-tech" Social Security Card. Proponents have denied that such a card is a biometric national ID card. Senator Schumer and Senator Graham, for example, have implied that a "high-tech" Social Security Card would not be a national ID card because "[e]ach card's unique biometric identifier would be stored only on the card; no government database would house everyone's information. The cards would not contain any private information, medical information or tracking devices. The card would be a high-tech version of the Social Security card that citizens already have." Schumer & Graham, *supra* note 38; *see also* FROOMKIN & WEINBERG, *supra* note 3.

185. A leaked copy of proposed legislation drafted by the White House was reported in the media on February 17, 2013. *See* Alan Gomez, *White House Immigration Plan Offers Path to Residency*, USA TODAY (Feb. 16, 2013, 10:06 PM), http://www.usatoday.com/story/news/nation/2013/02/16/obama-immigration-bill/1925017/.

186. Julia Preston, *Senators Offer a Bipartisan Blueprint for Immigration*, N.Y. TIMES, Jan. 28, 2013, at A1, *available at* http://www.nytimes.com/2013/01/28/us/politics/senators-

January 29, 2013,[187] it was agreed that the proposed legislation required the implementation of a more expansive digitalized national ID system. The Obama White House Proposal calls for a "fraud-resistant, tamper-resistant Social Security card" (i.e., a "high-tech Social Security Card").[188] The Bipartisan Senate Immigration Plan calls for "an effective employment verification system . . . through non-forgeable electronic means prior to obtaining employment,"[189] most likely the mandatory national expansion of E-Verify and/or a biometric-based E-Verify system.[190] Past legislative proposals recommending the national, mandatory expansion of E-Verify through the New Employee Verification Act,[191] for example, have recommended the development of a "high-tech Social Security Card" or a digitalized, biometric-driven method for identity verification pursuant to the E-Verify identity database screening system.[192]

More recently, on April 16, 2013, the U.S. Senate formally introduced the Bipartisan Senate Immigration Plan, entitled Border Security, Economic Opportunity, and Immigration Modernization Act.[193] This bill allocates $1 billion to the Social Security Administration to develop "fraud-resistant, tamper-resistant,

---

agree-on-blueprint-for-immigration.html; Ashley Parker, *Senators Call Their Bipartisan Immigration Plan a 'Breakthrough,'* N.Y. TIMES (Jan. 28, 2013), http://www.nytimes.com/2013/01/29/us/politics/senators-unveil-bipartisan-immigration-principles.html. The text of the 2013 Bipartisan Immigration Plan is available at http://www.nytimes.com/interactive/2013/01/23/us/politics/28immigration-principles-document.html.

187. Ezra Klein, *READ: President Obama's Immigration Proposal*, WASH. POST WONKBLOG (Jan. 29, 2013, 3:00 PM), *available at* http://www.washingtonpost.com/blogs/wonkblog/wp/2013/01/29/read-president-obamas-immigration-proposal/. The text of the White House 2013 Immigration Proposal is available at http://www.whitehouse.gov/the-press-office/2013/01/29/fact-sheet-fixing-our-broken-immigration-system-so-everyone-plays-rules.

188. Press Release, Office of the Press Sec'y, FACT SHEET: Fixing Our Broken Immigration System So Everyone Plays by the Rules (Jan. 29, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/01/29/fact-sheet-fixing-our-broken-immigration-system-so-everyone-plays-rules.

189. CHARLES SCHUMER, JOHN MCCAIN, DICK DURBIN, LINDSEY GRAHAM, ROBERT MENENDEZ, MARCO RUBIO, MICHAEL BENNET & JEFF FLAKE, BIPARTISAN FRAMEWORK FOR COMPREHENSIVE IMMIGRATION REFORM 4 (2013), *available at* http://www.c-span.org/uploadedFiles/Content/Documents/Bipartisan-Framework-For-Immigration-Reform.pdf. Both the 2013 Bipartisan Immigration Plan proposed by the Senate and the 2013 White House Immigration Proposal recommend the implementation of an electronic employment verification system. *See* Press Release, *supra* note 188.

190. *See* SCHUMER ET AL., *supra* note 189, at 4; *infra* notes 192, 196, 198.

191. H.R. 2028, 111th Cong. (2009).

192. *See id.*; Lora L. Ries, *B-Verify: Transforming E-Verify into a Biometric Employment Verification System*, 3 ALB. GOV'T L. REV. 271 (2010) (discussing "congressional commitment to E-Verify, including added improvements to the program, while Congress and [DHS] design the next generation of E-Verify, adding biometrics to the program"); *see also* Schumer & Graham, *supra* note 38.

193. S. 744, 113th Cong. (2013), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-113s744is/pdf/BILLS-113s744is.pdf (introduced on April 16, 2013) (Senators Charles Schumer (D-N.Y.), John McCain (R-Ariz.), Richard Durbin (D-Ill.), Lindsey Graham (R-S.C.), Robert Menendez (D-N.J.), Marco Rubio (R-Fla.), Michael Bennet (D-Colo.), Jeff Flake (R-Ariz.)).

wear-resistant, and identity theft-resistant social security cards."[194] The bill also requires the Secretary of DHS to explore the development of biometric-based IDs. Specifically, the bill states that "[n]ot later than 1 year after the date of the enactment of this Act" DHS must "submit a report to Congress on the feasibility, advantages, and disadvantages of including, in addition to a [digital] photograph, other biometric information on each employment authorization document issued by the Department."[195]

The bipartisan Senate bill further mandates the national expansion of E-Verify.[196] If the bill passes, under this E-Verify mandate, all employers, or nearly all employers, in the United States will be required to collect the personally identifiable data on all new employees (e.g., name, date of birth, and Social Security Number) and run this information over the Internet through government databases, in order to "verify" the employee's identity.[197] The bill also prescribes the creation of a universal, national digitalized photo database and, based upon this database, requires all employers to perform a primitive form of biometric analysis. E-Verify will require that all employers must inspect a digital photo, uploaded onto the Internet by the government through the E-Verify "Photo Tool," and compare the digital photo with the face of the individual seeking employment.[198]

---

194. *Id.* § 3102(a)(1)–(3), at 504–05.

195. *Id.* § 3103, at 509–10.

196. *See id.* § 3101(a), at 419 (amending language of Section 274A of the Immigration and Nationality Act of 1952 (INA), entitled Unlawful Employment of Aliens, to include establishment and implementation of an "Employment Verification System"). E-Verify was originally authorized as a "Basic Pilot Program" under the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, and its continuation as a test pilot program was subject to congressional reauthorization. Pub. L. No. 104-208, § 401, 110 Stat. 3009-546, 3009-655 to 3009-656 (codified at 8 U.S.C. § 1324a); *see also History and Milestones*, U.S. CITIZENSHIP & IMMIGRATION SERVS. (Mar. 18, 2013), http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=84979589cdb76210VgnVCM100000b92ca60aRCRD&vgnextchannel=84979589cdb76210VgnVCM100000b92ca60aRCRD. Thus, the repeal of the original authorization allows for the implementation of a mandatory and permanent E-Verify program. *See* S. 744, § 3101(a), at 503–04.

197. *See id.* The proposed legislation refers to the "System" and does not state explicitly that the system is E-Verify. However, the current digitalized "Employment Verification System" operated by DHS is E-Verify. The bill does not explain the specific mechanics of E-Verify in any detail, yet, does specify that "[t]he employer shall obtain from the individual (and the individual shall provide) and shall record in such manner as the Secretary may specify—(I) the individual's social security account number . . . [and] (III) such other information as the [DHS] Secretary may require to determine the identity and employment authorization of an individual." *Id.* at 429–30.

198. *See id.* at 412–13. The proposed legislation does not explain the specific details of how the E-Verify Photo Tool will work or how DHS will create a universal digitalized photo database of all prospective employees whose identities will be verified under the System. However, the bill seems to suggest that DHS intends to utilize digitalized driver's license photos from DMV photo databases, and other photo databases that may be maintained by state and local governments. *Id.* at 412 (requiring all states "to provide the [DHS] Secretary, for purposes of identity verification in the [E-Verify] System, with photographs and appropriate identifying information maintained by the State"). Next, the bill appears to require the development of a new USCIS database within DHS that incorporates state

If passed, the long-term implications of the bill on biometric data collection and biometric ID cybersurveillance and mass biometric dataveillance are likely to be significant. The bill does not indicate whether and which biometric identifiers will be included in the "high-tech" Social Security Card that the Social Security Administration has been tasked with implementing. The bill also does not indicate whether the E-Verify Photo Tool will utilize facial recognition technology. However, the Photo Tool likely necessitates the creation of a national digital photo database (a biometric database) for identification purposes (biometric database screening). Eventually, the "high-tech" Social Security Card and the E-Verify Photo Tool, or other technological evolutions of E-Verify that move towards biometric enhancements, will likely utilize some type of technological protocol that automates identification processes through biometric database screening and data matching technologies.

This comprehensive immigration reform proposal significantly increases the likelihood that a universal biometric database would need to be created. A universal digitalized biometric ID system would support the identity management systems already existing and that are expanded by the bill, as well as the new identity management programs and biometric ID enhancements that are proposed under the bill. In particular, the bill incorporates multiple provisions that include a dramatic expansion of both biometric data collection protocols and biometric database screening protocols.

Table 6 summarizes some of the ways in which the most recent comprehensive immigration reform bill emphasizes biometric data collection and screening as a significant component of immigration reform and border security policy.

Table 6. Examples of Biometric-Centered Provisions in the 2013 Bipartisan Senate Comprehensive Immigration Reform Bill: Border Security, Economic Opportunity, and Immigration Modernization Act (introduced April 16, 2013)

Title and Section	Section Name	Description
Title II, Section 2101[199]	Registered Provisional Immigrant Status[200]	Revises Immigration and Nationality Act of 1952 (INA) to include Section 245B, which sets up various requirements for granting registered provisional status and proposes to include a subsection on "Security and Law Enforcement Clearances" for registered provisional immigrants.[201] Sets forth requirement

biometric data (digitalized photos) and biographical data to facilitate E-Verify database screening. *Id.* at 413. Specifically, the bill directs the DHS Secretary to "develop and maintain a photo tool that enables employers to match the photo on a covered identity document provided to the employer to a photo maintained by a U.S. Citizenship and Immigration Services database." *Id.*

199. *Id.* § 2101, at 59–93.

200. *Id.*

201. *Id.* § 2101(a), at 78–79.

		to submit biometric and biographic data and pass background check.[202]
Title II, Section 2102[203]	Adjustment of Status of Registered Provisional Immigrants[204]	Revises INA to include Section 245C that establishes an application fee to cover processing costs, including cost of biometric and biographic data collection.[205]
Title II, Section 2103[206]	The DREAM Act[207]	Revises INA to include Section 245D, setting forth requirement to submit biometric and biographic data and pass background check.[208]
Title II, Section 2211[209]	Requirements for Blue Card Status[210]	Sets forth requirement for biometric and biographic data collection,[211] assessment of processing fee "to take and process biometrics,"[212] and denial of the application for failure to submit "requested biometric data."[213]
Title II, Section 2212[214]	Adjustment to Permanent Resident Status[215]	Sets forth requirement that application fee will cover "the cost of taking and processing biometrics."[216]
Title III, Section 3101[217]	Unlawful Employment of Unauthorized Aliens[218]	Amends Section 274A of the INA to include establishment and implementation of an "Employment Verification System" (e.g., mandating national implementation of E-Verify),[219] including mandatory

202. *Id.* at 78–85.
203. *Id.* § 2102, at 94–110.
204. *Id.*
205. *Id.* § 2102(a), at 94, 106.
206. *Id.* § 2103, at 110–17.
207. *Id.*
208. *Id.* § 2103(b), at 110, 113–14.
209. *Id.* § 2211, at 153–74.
210. *Id.* § 2211. "Blue Card Status" may be granted to an alien who "performed agricultural employment in the United States for not fewer than 575 hours or 100 work days during the 2-year period ending on December 31, 2010," and to such alien's spouse or child. *Id.* § 2211(a), at 153.
211. *Id.* § 2211(b)(6)(A), at 162.
212. *Id.* § 2211(b)(8)(A)(ii)(II), at 164.
213. *Id.* § 2211(b)(9)(A)(i), at 166.
214. *Id.* § 2212, at 174–84.
215. *Id.*
216. *Id.* § 2212(e)(2)(A)(i), at 179.
217. *Id.* § 3101, at 395–504.
218. *Id.*
219. *Id.* § 3101(a), at 395, 419–504.

		implementation of a "Photo Tool" (i.e., mandating the national expansion of digitalized photo database under the E-Verify "Photo Tool").[220]
Title III, Section 3102[221]	Increasing Security and Integrity of Social Security Cards[222]	Sets forth SSA's allocation of $1 billion to implement new Social Security Card,[223] and amends the Social Security Act to insert the following language: "'The social security card shall be fraud-resistant, tamper-resistant, wear-resistant, and identity theft-resistant.'"[224]
Title III, Section 3103[225]	Increasing Security and Integrity of Immigration Documents[226]	Section 3103 states: "Not later than 1 year after the date of the enactment of this Act, the [DHS] Secretary shall submit a report to Congress on the feasibility, advantages, and disadvantages of including, in addition to a photograph, other biometric information on each employment authorization document issued by the Department."[227]
Title III, Section 3304[228]	Identity-Theft Resistant Manifest Information for Passengers, Crew, and Non-Crew Onboard Departing Aircraft and Vessels[229]	Requires "biometric departure information" to be collected: "Carriers boarding alien passengers, crew, and non-crew subject to the requirement to provide information upon departure US-VISIT processing shall collect identity-theft resistant departure manifest information from each alien at a collection location at the airport or seaport before boarding

220. *Id.* at 413–15.
221. *Id.* § 3102, at 504–09.
222. *Id.*
223. *Id.* § 3102(a)(1)–(3), at 504–05. The proposed legislation does not use the words "high-tech" Social Security Card; however, as discussed above, previous discussions on the need to improve the Social Security Card have described such enhancements as "high-tech."
224. *Id.* § 3102(a)(2), at 505.
225. *Id.* § 3103, at 509–10.
226. *Id.*
227. *Id.*
228. *Id.* § 3304, at 543–48.
229. *Id.*

		that alien on transportation for departure from the United States."[230] Delegates to DHS Secretary determination of the appropriate method "to ensure the adequate collection and transmission of biometric departure manifest information."[231]
Title III, Section 3711[232]	Inadmissible Aliens[233]	Sets forth new ground for inadmissibility to include the failure to comply with biometric data collection request.[234]
Title IV, Section 4103[235]	Eliminating Impediments to Worker Mobility[236]	References "review of all standard database and biometric checks" in context of granting State Department ability to grant "Interview Waivers for Low Risk Visa Applicants."[237]

To understand part of the reason why the current immigration reform bill emphasizes the need for dramatically expanded biometric data collection and biometric database screening programs and protocols, it is useful to consider the current bill's predecessors. One recent predecessor, for example, was titled the Biometric Enrollment, Locally-stored Information, and Electronic Verification of Employment (BELIEVE) proposal, and was introduced in 2010.[238] The BELIEVE proposal was unlike other biometric ID data collection programs that have been previously implemented—such as Homeland Security Presidential Directive 12 (HSPD-12), United States Visitor and Immigrant Status Indicator Technology (US-VISIT), and the DNA Fingerprint Act of 2005—which limited the collection of biometric data to discrete subsets of the U.S. population. In contrast, recent immigration reform and identity management proposals, such as BELIEVE and the 2013 Bipartisan Senate Comprehensive Immigration Reform Bill, recommend a universal or near-universal collection of biometric data—such as digital photos,

230. *Id.* § 3304(b)(3), at 544–45.
231. *Id.* § 3304(e), at 547.
232. *Id.* § 3711, at 633–38.
233. *Id.*
234. *Id.* § 3711(b)(1), at 634.
235. *Id.* § 4103, at 664–67.
236. *Id.*
237. *Id.* § 4103(d), at 666–67.
238. *See* REPAIR, *supra* note 184, at 11–18; *see also* Ezra Klein, *Is a Biometric, National ID Card an Immigration Game Changer?*, WASH. POST.COM (Apr. 30, 2010, 10:45 AM), http://voices.washingtonpost.com/ezra-klein/2010/04/is_a_biometric_national_id_car.html; FROOMKIN & WEINBERG, *supra* note 3; Schumer & Graham, *supra* note 38, ("We would require all U.S. citizens and legal immigrants who want jobs to obtain a high-tech, fraud-proof Social Security Card. Each card's unique biometric identifier would be stored only on the card . . . .").

scanned fingerprints and irises, and/or DNA—from every U.S. citizen and noncitizen currently residing in the United States,[239] over 300 million men, women, and children, according to the U.S. Census.[240]

In BELIEVE, for example, Congress recommended replacing the paper-based Social Security Card with a digitalized national biometric ID,[241] also referred to as a "high-tech, fraud-proof Social Security Card."[242] The BELIEVE immigration reform proposal recommended collecting and including biometric data and other personally identifiable data on a machine-readable card.[243] Policymakers explained that the "high-tech Social Security Card" would operate similarly to a credit card in a machine-swipe capacity.[244] Unclear in the BELIEVE proposal was whether such a "high-tech" Social Security Card would include a geolocational tracking device. The surveillance capacity of a device that resembles a credit card is significant in part because "there is now a [GPS] device in use that weighs two ounces and is the size of a credit card."[245] Therefore, geolocational tracking through a "high-tech" Social Security Card that resembles a credit card could be made possible through GPS, RFID, or a combination of GPS-RFID technologies.[246]

Calls for a national biometric ID have also been made in connection with state immigration reform efforts such as those passed in Arizona. For example, immediately after passage of the highly controversial Arizona Senate Bill 1070 (SB 1070), one member of Congress declared on national television, "I'm ready to give a little blood and a little DNA to prove that I'm legally working in the United States of America," protesting both Arizona's presumptive racial profiling mandate and the current "broken" immigration system.[247] The congressman elaborated that a biometric-based, high-tech Social Security Card was essential to fixing the immigration system. Moreover, the "architect of Arizona immigration law SB 1070"[248] has argued that biometric passports are necessary to "secure the

---

239. *See, e.g.*, Danny Yadron, *Senators in Immigration Talks Mull Federal IDs for All Workers*, WALL ST. J., Feb. 21, 2013, at A1, *available at* http://online.wsj.com/article/SB10001424127887323864304578316434045924350.html ("Key senators are exploring an immigration bill that would force every U.S. worker—citizen or not—to carry a high-tech identity card that could use fingerprints or other personal markers to prove a person's legal eligibility to work.").

240. *U.S. & World Population Clock*, U.S. CENSUS BUREAU, *available at* http://www.census.gov/popclock/ (as of May 6, 2013, the U.S. Census reports 315,808,633 in the U.S. population).

241. *See* Schumer & Graham, *supra* note 38.

242. *Id.*

243. *See id.*; *see also* REPAIR, *supra* note 184, at 8–11.

244. Schumer & Graham, *supra* note 38 ("Prospective employers would be responsible for swiping the cards through a machine to confirm a person's identity and immigration status.").

245. United States v. Jones, 132 S. Ct. 945, 957 n.1 (2012) (Alito, J., concurring).

246. *See supra* note 150.

247. Lynn Sweet, *Gutierrez Arrested for Immigration Protest; Explains on CBS "Face the Nation,"* CHI. SUN-TIMES (May 2, 2010, 8:19 PM), http://blogs.suntimes.com/sweet/2010/05/gutierrez_arrested_for_immigra.html (transcribing a Face the Nation interview with Congressman Luis Gutierrez (D-Ill.)).

248. John Hanna, *Kris Kobach, Architect of Arizona Immigration Law SB1070, Is Behind*

border" and verify the identity of those in the U.S. who may be potential terrorists.[249] Consequently, both opponents and proponents of Arizona SB 1070 have called for the implementation of a digitalized biometric ID for immigration reform purposes.

Further, although proponents of such a measure contend that a "high-tech" Social Security Card is not a "Biometric National ID Card,"[250] experts have already concluded that such a "high-tech" card or cardless system such as E-Verify would function as a national ID[251] given that the Social Security Number has transformed from its original intended function.[252] Although established in the 1930s as a government-assigned number intended to facilitate the transmission of a federal retirement benefit, experts have observed that the Social Security Number has morphed into a universal de facto national ID number.[253]

Currently, the Social Security Number provides an essential universal data "backbone identification tool" for many identity management programs and database screening systems. E-Verify and the Help America Vote Act (HAVA) database screening protocols, for example, rely upon this data backbone.[254] Identity management technologies such as E-Verify and HAVA both depend on the Social Security Number to determine whether there is a "match" between the person presenting the data and the preexisting Social Security Administration (SSA) database.[255] The statistical algorithms of the E-Verify software program necessitate,

---

Other Controversial Laws (May 10, 2010, 5:41 PM), http://www.huffingtonpost.com/2010/05/10/kris-kobach-architect-of_n_570662.html.

249. *See Comprehensive Immigration Reform in 2009, Can We Do It and How?: Hearing Before the Subcomm. on Immigration, Border Sec. and Refugees of the S. Comm. on the Judiciary*, 111th Cong. 34 (2009) [hereinafter Comprehensive Immigration Reform 2009 Hearings] (testimony of Kris W. Kobach, Professor of Law, Univ. of Mo. (Kan. City) Sch. of Law), *available at* http://www.judiciary.senate.gov/pdf/09-04-30KobachTestimony.pdf.

250. *See* Schumer & Graham, *supra* note 38.

251. Harper, *supra* note 26. Former Congressman Bob Barr (R-GA) observes that E-Verify functionally operates as a "stealth" national ID system under the definition set forth by Jim Harper. *See* Bob Barr, *"E-Verify" Is a Stealth National ID*, THE BARR CODE (June 10, 2011, 5:00 AM), http://blogs.ajc.com/bob-barr-blog/2011/06/10/e-verify-is-a-stealth-national-id/; *see also* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE REAL ID ACT 5 (2007) [hereinafter REAL ID PRIVACY IMPACT ASSESSMENT], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf ("An argument exists that both the SSN and existing state credentials already create *de facto* national identifiers.").

252. ELEC. PRIVACY INFO. CTR., REAL ID IMPLEMENTATION REVIEW: FEW BENEFITS, STAGGERING COSTS 1–3 (2008), available at http://epic.org/privacy/id_cards/epic_realid_0508.pdf.

253. *See id.*

254. Cate, *supra* note 34, at 469 (describing the Social Security Administration's NUMIDENT database as the "backbone identification verification tool for social service and other federal programs"). HAVA mandates states to conduct database screening on the driver's license number or the last four digits of the Social Security Number to authenticate the identity of newly registered voters. 42 U.S.C. § 15483(a)(5)(A)(i)(I)−(II) (2006).

255. *See E-Verify: Preserving Jobs for American Workers: Hearing Before the Subcomm. on Immigration Policy and Enforcement of the H. Comm. on the Judiciary*, 112th Cong. 27–28 (2011) (written testimony of Theresa C. Bertucci, Associate Director, Enterprise Services Directorate, U.S. Citizenship and Immigration Services); Carolyn Puckett, Office of

therefore, the collection of an employee's Social Security Number, if such a number exists.

As a de facto national ID number,[256] the Social Security Number is used to track and screen data on individuals for multiple purposes.[257] But the susceptibility of the Social Security Number to fraudulent misuse is precisely why policymakers are now looking to biometric data. In recent years, both public and private sector leaders have expressed concern that the Social Security Number is not reliable enough as a data "backbone" to support identity management systems.[258] In short, there are too many anomalous results from the Social Security Number database and the identity verification matching technologies that rely upon a Social Security Number as a data backbone. The statistical algorithms needed to support identity verification thus require more and more additional personally identifiable data to increase the reliability that an individual is a true "match" in the database screening process by comparing present data with preexisting database information.[259] Consequently, policy experts are calling for multimodal biometric identification systems (a combination of facial recognition, fingerprints, iris scans, and DNA, for instance) to serve as the new data backbone to increase the reliability of identity screening systems.[260]

Retirement and Disability Policy, *The Story of the Social Security Number*, 69 SOC. SEC. BULL., no. 2, 2009, at 55, 69–70.

256. REAL ID PRIVACY IMPACT ASSESSMENT, *supra* note 251, at 5 (noting that the Social Security Number has become a "de facto" national identification number, and that "it is yet unclear whether a REAL ID compliant driver's license or identification card will become any more of a national ID than the Social Security Number (SSN) or existing state-issued driver's licenses and identification cards.").

257. *Id.* at 6 ("Thus, for example, if retailers, healthcare providers, financial institutions, insurers, and other private or government entities were to collect the credential and record the ID number whenever individuals engaged in a transaction, the REAL ID's unique number could pose the same, if not greater, risks as experienced in the use of the SSN." (footnote omitted)).

258. Cate, supra note 34, at 469 (observing that the error rate of SSA's NUMIDENT database was found to be 4.1%—in other words, 17.8 million records "contained 'discrepancies in the name, date of birth or citizenship status of the numberholder' or concerned deceased individuals" (quoting Office of Inspector Gen., Soc. Sec. Admin., Congressional Response Report: Accuracy of the Social Security Administration's NUMIDENT File (A-08-06-26100), at ii (2006))).

259. Identity management programs such as E-Verify rely upon algorithmic data matching technologies. *See, e.g.*, GAO EMPLOYMENT VERIFICATION, *supra* note 109. Like many new identity management systems that rely upon statistical algorithms, these data-driven systems and big data are "about applying math to huge quantities of data in order to infer probabilities . . . . The key is that these systems perform well because they are fed with lots of data on which to base their predictions." MAYER-SCHÖNBERGER & CUKIER, *supra* note 31, at 11–12.

260. *See, e.g.*, LYNCH, *supra* note 3, at 10 ("Traditionally, biometrics databases such as IAFIS and IDENT have collected only one biometric at a time [e.g., fingerprints]. However, the government has argued these 'unimodal' systems are limited and has been pushing to develop 'multimodal' systems that collect and combine two or more biometrics (for example, photographs and fingerprints). The government argues that collecting multiple biometrics from each subject will make identification systems more accurate." (footnotes omitted)); *see also* GAO TECHNOLOGY ASSESSMENT, *supra* note 3, at 58; Janice Kephart,

Once implemented, a more comprehensively invasive biometric-based universal data backbone (rather than Social Security Number-based data backbone) could be utilized to analyze data on any given individual through data mining and profiling. Already, government and government-contracted data aggregation systems analyze data from publicly available databases and private data and databases. "Much of the data is collected from electronic surveillance and documents obtained by government agencies or in collaboration with commercial sources."[261] These commercial and government sources can be aggregated to develop "transactional history [that] shows employment status, credit history, use of government services, travel patterns, financial transactions, and consumer habits that when combined depict the person's identity and overall activities."[262]

Currently, in addition to an individual's name, one's birthdate, Social Security Number, and other numbers (driver's license, passport, etc.) are used to facilitate this type of database sorting. Adding biometric data enhancements to a numerical data backbone, such as the Social Security Number, risks even greater government intrusiveness because of the sensitive information that can be gleaned from an individual's DNA (genetic disorders, behavioral genetic profiling, religious and ethnic heritage, etc.) as well as information that can be analyzed from other biometric data, such as information yielded by a digital photo (demographic information such as race and color as well as digitalized facial analytical profiling).[263]

B. Portability of Biometric Screeners and Mobile Biometric Sensors

The feasibility of utilizing biometric data as a form of mass identification, rather than relying upon an identifier such as the Social Security Number, has been greatly enhanced by the emerging development of portable, noninvasive biometric screeners (e.g., devices that can collect and screen biometric data through databases) and mobile biometric sensors (e.g., devices that can capture and enroll biometric data in biometric databases). Policy trends in recent years have

---

Border Watchlisting a Decade After 9/11, CTR. FOR IMMIGRATION STUD. (Aug. 2011), http://www.cis.org/border-watchlisting-9-11 ("To ensure a more accurate watchlist, biometrics, including digitized facial images and fingerprints, need to be fully incorporated into watchlisting."); *Written Testimony of U.S. Customs and Border Protection Border Patrol Chief Michael Fisher, Office of Field Operations Assistant Commissioner Kevin McAleenan, and Office of Technology Innovation and Acquisition Assistant Commissioner Mark Borkowski for a House Committee on Homeland Security, Subcommittee on Border and Maritime Security: "Measuring the Outcomes To Understand the State of Border Security,"* U.S. DEP'T OF HOMELAND SEC. (Mar. 20, 2013) [hereinafter *Measuring the Outcomes*], http://www.dhs.gov/news/2013/03/20/written-testimony-cbp-house-homeland-security-subcommittee-border-and-maritime; Simone Wilson, *FBI Documents Reveal ICE's 'Secure Communities' Program Was Mandated To Further FBI's Own Creepy Biometric Database*, LA WEEKLY BLOGS (Jul. 6, 2011, 9:30 AM), http://blogs.laweekly.com/informer/2011/07/fbi_documents_ice_secure_communities_program_mandated_biometric_database.php.

261. BLOSS, *supra* note 92, at 181.

262. *Id. See generally* GARFINKEL, *supra* note 3; O'HARROW, *supra* note 3; PRIEST & ARKIN, *supra* note 13.

263. *See generally* TROY DUSTER, BACKDOOR TO EUGENICS (2003).

increasingly emphasized the need for portable and handheld biometric screeners and mobile biometric sensors. These newly developed technologies facilitate the ability to use biometric-based data backbones as a method to augment and/or replace a Social Security Number-based data backbone.

Table 7 provides examples of the proliferation of the use of portable biometric screeners that allow for the collection and analysis of biometric data in the field.

Table 7. Examples of Portable and Handheld Biometric Screeners

Program	Entity	Description	Biometric Data
Portable DNA Screeners (DHS Test Pilot)	DHS/Network Biosystems[264]	"DHS responsibilities such as granting asylum, processing applications for relatives to come to the U.S., and deterring child trafficking and illegal adoptions can be enhanced significantly."[265]	DNA
Mona Passage Proof of Concept	US-VISIT/U.S. Coast Guard	"Handheld devices obtained fingerprint and digital images, connecting biometric information with biographic data (name, gender, date of birth, nationality, departure point, date of departure, destination point, and identity of the master of the U.S. vessel in question)" to provide biometric analysis and collection capabilities at sea.[266]	Fingerprints and digital photographs[267]
Secure Electronic	CrossMatch Technologies[268]	A 3.6 pound unit that enrolls biometric data	"Combin[es] forensic-quality

264. Mickey McCarter, *Homeland Security Considering Portable, Instant DNA Scanners*, FOX NEWS (Mar. 4, 2011), http://www.foxnews.com/tech/2011/03/04/homeland-security-considering-portable-instant-dna-scanners/.

265. *Id.*

266. Donohue, *supra* note 3, at 482 (footnote omitted).

267. *Id.*

Enrollment Kit (SEEK II)		into AFIS databases, such as DoD ABIS, and leverages a 120,000-person watchlist; designed for "rugged" use.[269]	fingerprint capture, rapid dual iris scan capability and innovative facial capture technology."[270]
HIIDE (Handheld Interagency Identity Detection Equipment)	U.S. Army[271]	Reportedly used for border security in Afghanistan. "The handheld device can store up to 22,000 profiles[.]"[272]	Fingerprint scans, iris scans, and facial recognition technology[273]

With a universal biometric database and "cardless" national ID system, such as a biometric E-Verify system, or biometric national ID card—e.g., digitalized and multimodal biometric driver's license, Social Security Card, or passport—federal, state, and local law enforcement could scan biometric data or request to see a digitalized biometric ID for a wide range of reasons, including routine traffic stops.[274] With a biometric identifier extracted from one's body—for instance, by digitally scanning one's face, fingerprints, irises; and/or swabbing saliva for DNA profiling—law enforcement could run this information against biometric databases in an attempt to authenticate or determine identity. Such mass biometric dataveillance programs could eventually be used to serve identity inference systems and big data cybersurveillance technologies as well.

---

268. CROSSMATCH TECHNOLOGIES, SEEK II (June 25, 2012), *available at* http://www.crossmatch.com/product_assets/brochures/SEEKII.pdf.

269. *Id.*

270. *Id.*

271. Richard Andrade, *Troopers Deploy HIIDE System at Border Crossing Point*, U.S. ARMY (Feb. 12, 2011), http://www.army.mil/article/51768/troopers-deploy-hiide-system-at-border-crossing-point/.

272. *Id.*

273. *Id.*

274. The Court has upheld the constitutionality of state statutes requiring suspects to "identify themselves" during police investigations. *See* Hiibel v. Sixth Judicial District Court of Nevada, 542 U.S. 177 (2004) (holding that law enforcement's legitimate need to dispel suspicion of criminal activity justified requiring self-identification by a suspect during *Terry* stops under the rubric of *Terry v. Ohio*, 392 U.S. 1 (1968), and that the state statute's requirement of self-identification did not violate the Fifth Amendment, however, leaving open the potential that providing a name could be self-incriminating and may implicate the Fifth Amendment in another factual circumstance); United States v. Brignoni-Ponce, 422 U.S. 873 (1975) (holding that U.S. Border Patrol may stop vehicles near the U.S.-Mexico border and query citizenship and immigration status of vehicle occupants who appear to be of Mexican national origin, combined with other facts and inferences that raise reasonable suspicion regarding legal immigration status of those questioned); *see also* Kevin R. Johnson, *How Racial Profiling in America Became the Law of the Land:* United States v. Brignoni-Ponce *and* Whren v. United States *and the Need for Truly Rebellious Lawyering*, 98 GEO. L.J. 1005 (2010).

Table 8 indicates that smartphone technology, in particular, is facilitating methods by which the public and private sectors can track and verify biometric and biographic data simultaneously.

Table 8. Examples of Smartphones as Mobile Biometric Screeners and Sensors

Program	Entity	Description
Tactivo[275]	Precise Biometrics	Device is a "combination smart card and fingerprint reader for iPhone 4 and 4S." It is an identity verification system that supports the use of government credentials, such as CAC, PIV, and TWIC.[276]
Mobile Offender Recognition and Information System (MORIS)	BI^2 Technologies	Hardware attachment and software application for smartphones allows police officers to identify suspects using iris recognition, fingerprints, and digital photographs.[277] Application links to a national database of criminal records managed by BI^2 Technologies.[278]
eyeD Biometric Password Manager	Winkpass Creations, Inc.	Application compatible with iPhones uses your iris scan as your password for secure information.[279]

275. The federal government ordered Tactivo in August of 2012. Jill Jaracz, *U.S. Government Orders Tactivo Smart Casings*, SECUREIDNEWS (Aug. 7, 2012), http://www.secureidnews.com/2012/08/07/u-s-government-orders-tactivo-smart-casings.

276. *Mobile Device Security with Tactivo*, PRECISE BIOMETRICS, http://www.precisebiometrics.com/tactivo-for-government. Tactivo matches smart card credentials with the fingerprint application on the iPhone, acting almost as a handheld E-verify system. *See id.*

277. *BI2 Technologies MORIS*, POPSCI.COM, http://www.popsci.com/bown/2010/product/b12-technologies-moris.

278. Emily Steel, *How a New Police Tool for Face Recognition Works*, WALL ST. J. BLOGS (July 13, 2011, 7:56 AM), http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/.

279. *eyeD® Biometric Password Manager*, ITUNES, https://itunes.apple.com/us/app/eyed-biometric-password-manager/id389295175?mt=8.

C. Government Biometric Databases and Database Screening Programs

Federal and state governments operate multiple biometric databases and are increasingly emphasizing the need to collect biometric data and to screen this data through biometric databases. With the ease of a scan by a smartphone (e.g., fingerprint and iris scan) and with a card swipe or a tap of a smartphone against another smartphone or portable screener, law enforcement could instantly compile a "detailed digital dossier"[280] from a search of multiple public and private databases. Applying the "No-Fly List" practice to a more universal application, law enforcement could use an algorithm-based threat risk assessment to justify the search and detention of those stopped. Given current trends in DNA-based prosecutions, evidence from a database search could potentially lead to arrest and conviction based on "cold hit" DNA database evidence alone.[281]

Table 9 provides examples of federal and state biometric databases that currently store biometric data for identity verification database screening and other purposes.

Table 9. Examples of Government Biometric Database Programs

Program	Entity	Description
Combined DNA Index System (CODIS)[282]	FBI	Federal and state combined DNA database containing DNA from over 10 million profiles, collected during ongoing state criminal investigations.[283] "CODIS software makes it possible for local, state and federal crime laboratories to share and compare DNA data."[284]
National DNA Index System (NDIS)[285]	FBI	Federal DNA database[286]

280. GARFINKEL, *supra* note 3, at 70; *see also* Solove, *supra* note 21.

281. *See* Roth, *supra* note 29.

282. Authorized by the DNA Identification Act of 1994, 42 U.S.C. § 14132 (2006).

283. *CODIS—NDIS Statistics*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/lab/codis/ndis-statistics (over 10 million offender profiles as of March 2013, and FBI reports that CODIS has produced over 205,700 hits assisting in more than 197,400 investigations).

284. Anna Stolley Persky, *An Arresting Development: Courts Split Over DNA Testing for Those Merely Charged with a Crime*, 98 A.B.A. J. MAG., Jan. 1, 2012, at 15.

285. Authorized by the DNA Identification Act of 1994, 42 U.S.C. § 14132 (2006).

286. *See Frequently Asked Questions (FAQs) on the CODIS Program and the National DNA Index System*, FED. BUREAU INVESTIGATION, http://www.fbi.gov/about-us/lab/codis/codis-and-ndis-fact-sheet.

Integrated Automated Fingerprint Identification System (IAFIS)	FBI	Fingerprint database[287]
Automated Biometrics Identification System (ABIS)	U.S. Department of Defense (DoD)	To enable military agencies to conduct automated fingerprint searches.[288]
Automated Biometric Identification System (IDENT)	DHS	Database of digital photos and fingerprints[289]
Next Generation Identification (NGI)	FBI	Interoperable, centralized, and technologically compatible biometric data system across federal, state, and military operations and databases.[290]
DoD Next Generation ABIS	DoD	Designed to identify "persons of national security interest"[291] for force protection, including "'operational encounters, base access, and detainee management.'"[292]
ABIS (includes Watchlist Gallery database and Passport	DoS	Worldwide facial recognition system run by DoS to evaluate visa

287. *See Integrated Automated Fingerprint Identification System*, FED. BUREAU INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis.

288. *See* BIOMETRICS TASK FORCE, ANNUAL REPORT FY07 6 (2007), *available at* http://www.biometrics.dod.mil/Files/Documents/AnnualReports/fy07.pdf.

289. *See* IDENT PRIVACY IMPACT ASSESSMENT, *supra* note 120, at 3.

290. *See Next Generation Identification*, FED. BUREAU INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi; FED. BUREAU INVESTIGATION, PRIVACY IMPACT ASSESSMENT INTEGRATED AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (IAFIS)/NEXT GENERATION IDENTIFICATION (NGI) BIOMETRIC INTEROPERABILITY (2012), *available at* http://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngi-interoperability-1.

291. Donohue, *supra* note 3, at 452.

292. *Next Generation ABIS Goes Operational, Now Referred to as DoD ABIS*, BIOMETRICS TASK FORCE, http://www.biometrics.dod.mil/Newsletter/issues/2009/Apr/v5issue2_a1.html (quoting Mark Downs, DoD Abis Operations Mgr. for the Biometrics Task Force).

Lookout Tracking System)[293]		and passport applications.[294]
Consular Consolidated Database (CCD)	DoS	Data warehouse that stores biometric and biographic information on U.S. citizens, lawful permanent residents, and foreign nationals to screen visa applicants, register facial images, and report on particular applicants.[295]
Biometric Storage System	USCIS	"[C]entralized repository of all biometric data captured by USCIS from applicants filing immigration applications."[296]
TECS System ("CBP Primary and Secondary Processing (TECS) National SAR [Suspicious Activity Reports] Initiative")[297]	U.S. Customs and Border Protection (CBP)[298]	Data repository for U.S. CBP database screening: "TECS is the principal system used by officers at the border to assist with screening and determinations regarding admissibility of arriving persons."[299]
Interstate Photo System	FBI	Component of NGI that

293. U.S. DEP'T OF STATE, PRIVACY IMPACT ASSESSMENT: PASSPORT LOOKOUT TRACKING SYSTEM (PLOTS) PIA (2012), *available at* http://www.state.gov/documents/organization/109088.pdf; U.S. DEP'T OF STATE, AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS) PRIVACY IMPACT ASSESSMENT 1 (2011) [hereinafter ABIS PRIVACY IMPACT ASSESSMENT], *available at* http://www.state.gov/documents/organization/109132.pdf.

294. ABIS PRIVACY IMPACT ASSESSMENT, *supra* note 293.

295. Donohue, *supra* note 3, at 435–36. The CCD does not directly collect information from individuals and thus does not have to provide notice in accordance with the Privacy Act. *See* U.S. DEP'T OF STATE, CONSULAR CONSOLIDATED DATABASE (CCD) PRIVACY IMPACT ASSESSMENT (PIA) 17 (2010), *available at* http://www.state.gov/documents/organization/93772.pdf.

296. Donohue, *supra* note 3, at 435 (footnote omitted).

297. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING (TECS) NATIONAL SAR INITIATIVE 2 (2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs-sar-update.pdf. TECS was formerly known as the Treasury Enforcement Communications System. *Id.*

298. *Id.*

299. *Id.*

(IPS)		incorporates media not just from law enforcement but from private businesses, social networking sites, government agencies, and foreign and international entities, as well as individuals like acquaintances, friends, and family members.[300]
DNA collection of convicted offenders and those arrested or charged[301]	States and the federal government[302]	Twenty-eight states and the Federal government authorize the collection of DNA from those arrested or charged with certain qualifying offenses.[303]
DNA collection from juvenile arrestees	States	Thirty states collect DNA from juveniles.[304]

300. *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, FED. BUREAU INVESTIGATION (June 9, 2008), http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system. The media stored by the system includes photographs searchable by using facial recognition technology, as well as photographs of scars, distinct marks, and tattoos. *See Next Generation Identification*, *supra* note 290.

301. Thirteen of the twenty-eight states collect DNA from all those arrested for a felony; the others limit collection to certain felonies, usually those involving violence or sexual assault. Julie Samuels, Elizabeth Davies, Dwight Pope & Ashleigh Holand, *Collecting DNA from Arrestees: Implementation Lessons*, NAT'L INST. OF JUSTICE, no. 270, June 2012, at 18, 21. Seven states collect from those arrested or charged with misdemeanors. *Id.*

302. "Most states place the responsibility for initiating expungement on the individual from whom a sample was collected. States that bear the responsibility for initiating expungement include Maryland, Missouri, North Carolina, South Carolina, Tennessee, Vermont and Virginia." *Id.* at 23 (footnote omitted).

303. *Id.* at 19. "The pace of expansion increased dramatically after Congress passed the DNA Fingerprint Act of 2005, which, among other things, enabled states to upload arrestee DNA profiles to the National DNA Index System (NDIS). Between 2006 and 2011, 23 states passed arrestee DNA collection legislation." *Id.* (footnote omitted). Of the twenty-eight states that authorize the collection of DNA from those arrested or charged with certain qualifying offenses, only eleven require a judicial determination prior to DNA collection. *Id.* at 20 fig. 1.

304. JULIE E. SAMUELS, ALLISON M. DWYER, ROBIN HALBERSTADT & PAMELA LACHMAN, URBAN INSTIT. JUSTICE POL'Y CTR., COLLECTING DNA FROM JUVENILES iii (2011), *available at* http://www.urban.org/UploadedPDF/417487-Collecting-DNA-from-Juveniles.pdf. But, only ten of these states provided "meaningful data on juvenile profiles in state or national databases." *Id.* at v. Of these ten states, which represented 42% of the total number of

Additionally, a "high-tech" Social Security Card, such as the one promulgated under BELIEVE and now contemplated for further exploration by the Social Security Administration under the 2013 Bipartisan Senate Comprehensive Immigration Reform Bill, likely would have a significant impact on existing "stop and identify yourself" laws and programs.[305] State and local law enforcement agencies, in partnership with the federal government, have increasingly incorporated elements of database screening technologies, including biometric database screening protocols.[306] Consequently, the proponents of immigration federalism—state and local government efforts to control unwanted migration—have specifically called for the implementation of a biometric ID.[307] A biometric national ID card would greatly facilitate the database screening protocols required by various dataveillance tools embedded within biometric data screening protocols mandated by immigration federalism laws.[308]

Table 10 provides examples of identity-verification programs that utilize database screening protocols as a method of immigration and crime control enforcement.

Table 10. Examples of Immigration-Related Biometric Screening Programs

Program	Entity	Description
Secure Communities (S-COMM)	U.S. Immigration and Customs Enforcement (ICE)	Fingerprint-based arrest protocol requiring biometric database screening of anyone apprehended by state and local law enforcement through DHS and FBI databases.[309]
Criminal Alien Program (CAP)	ICE/FBI	Cooperating state and local jails, prisons, and detention facilities allow federal immigration agents to conduct

profiles uploaded to CODIS that collect juvenile DNA, "juvenile profiles accounted for six percent of all DNA profiles submitted." *Id.*

305. *See, e.g.*, Hiibel v. Sixth Judicial District Court of Nevada, 542 U.S. 177 (2004) (holding that state "stop and identify" statutes do not violate Fourth Amendment).

306. *See* Donohue, *supra* note 3, at 460–61; RANDY CAPPS, MARC R. ROSENBLUM, CRISTINA RODRIGUEZ & MUZAFFAR CHISHTI, MIGRATION POLICY INST., DELEGATION AND DIVERGENCE: A STUDY OF 287(G) STATE AND LOCAL IMMIGRATION ENFORCEMENT 17 (2011); *supra* Part I.B.2; *infra* note 332.

307. *See, e.g.*, Comprehensive Immigration Reform 2009 Hearings, *supra* note 249, at 34 (testimony of Kris W. Kobach, Professor of Law, Univ. of Mo. (Kan. City) Sch. of Law); *see also* Hanna, *supra* note 248 (describing Kobach as the "architect" of Arizona's immigration law, SB 1070).

308. *See, e.g.*, Hu, *supra* note 13, at 596–604.

309. *See Secure Communities*, *supra* note 131.

		biometric database (fingerprint-based) screening onsite through DHS and FBI databases.[310]
National Crime Information Center (NCIC)	FBI	FBI criminal database that is used for S-COMM immigration screening, including biometric screening.[311]
United States Visitor and Immigrant Status Indicator Technology (US-VISIT)	USCIS	Requires biometric data collection from all noncitizen visitors to the United States.[312]

III. DIGITALIZED BIOMETRIC DATA AND BIOMETRIC DATA MATCHING

Proponents of a biometric national ID champion the creation of a national identification credentialing database, supported by the development of a universal data backbone based upon traditionally gathered personally identifiable information, as well as newly acquired biometric data.[313] Moreover, the multiplicity of identity management programs, often requiring the collection of varying personally identifiable information, creates unifying pressure to develop a single universal data backbone.[314] Given this, it is important to understand the mechanics of biometric data collection and matching. It is equally important to understand the problems and concerns that have been raised about biometric identification management systems.

A. Biometric Data Collection

Biometric IDs and the surveillance they enable require as an initial matter the collection of biometric data from individuals. Biometric data is alluring for security purposes because it appears forgery resistant insofar as the data comes from one's

310. *See Fact Sheet: Criminal Alien Program (CAP)*, U.S. IMMIGRATION & CUSTOMS ENFORCEMENT (Mar. 29, 2011), http://www.ice.gov/news/library/factsheets/cap.htm.

311. *See National Crime Information Center*, FED. BUREAU INVESTIGATION, http://www.fbi.gov/about-us/cjis/ncic. NCIC database is used for multiple purposes and is accessible by law enforcement agencies nationwisde. *Id.*

312. *See Fact Sheet: US-VISIT Program*, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (May 19, 2003), http://www.ice.gov/news/library/factsheets/us-visit.htm.

313. *See, e.g.*, Jim Harper, *Schumer and Graham on Immigration Reform: Why Not Do It Without the Biometric National ID?*, CATO AT LIBERTY BLOG (Mar. 19, 2010, 9:45 AM), http://www.cato.org/blog/schumer-graham-immigration-reform-why-not-do-it-without-biometric-national-id (arguing that although Schumer and Graham claim that their proposal for a biometric national ID would not include a government database, that is the natural result of their plan).

314. *Id*.

own body. As discussed above, digitalized biometric data is currently defined as information that provides a unique technological identifier based on an individualized characteristic of one's body.[315] Biometric data currently can be pulled, for example, from fingerprint and iris scans, DNA, skeletal bone imaging, facial recognition software through digital photographs, and voice recognition software through voice recordings.[316]

In Tables 11 through 13, I provide common examples of various biometric data harvesting programs: DNA data collection, fingerprint data collection, and digitalized facial recognition data collection. As the tables make clear, the harvesting of bodily data is already widespread and routine, even as it is also evolving and expanding in terms of the kinds of government programs that mandate it. Those suspected of criminal or otherwise unlawful presence in the country are currently targeted by government biometric data harvesting programs.[317] However, I also include private ID programs below to show that the surrender of such data is becoming normalized by, for example, amusement parks, banks, and health clubs.

Table 11. Examples of DNA Data Harvesting Programs

Program	Entity	Description
DNA Analysis Backlog Elimination Act of 2000[318]	FBI	Compels production of DNA samples from parolees of qualifying federal offenses.[319]
Katie Sepich Enhanced DNA Collection Act of 2010[320]	FBI	Compilation of national DNA databases taken from people arrested of crimes (does not require conviction for DNA data harvesting).[321]

315. BIOMETRIC RECOGNITION, *supra* note 3, at 1–4.

316. *See, e.g.*, VACCA, *supra* note 3; BIOMETRIC RECOGNITION, *supra* note 3, at 31–34.

317. *See, e.g.*, *Secure Communities*, *supra* note 131; *Fact Sheet: US-VISIT Program*, *supra* note 312.

318. Pub. L. No. 106-546, 114 Stat. 2726 (2000) (codified as amended at 42 U.S.C. §§ 14135–14135e (2006); 10 U.S.C. § 1565 (2006)).

319. *See* 42 U.S.C. § 14135a(a)(2).

320. H.R. 4614, 111th Cong. (2010).

321. *Id.*

"Juli's Law"[322] and other state DNA harvesting laws.[323]	Under many of the state laws requiring DNA harvesting, DNA saliva swabbing kits are provided to state prisons and local jails where samples are collected.[324] The information gathered often includes offenders' names, Social Security Numbers, birth dates, signatures, federal or state offender identification numbers, and fingerprints.[325]	DNA collection of those detained for felony and misdemeanor offenses of assault and battery, domestic abuse, stalking, possession of a controlled dangerous substance, outraging public decency, resisting arrest, and peeping Tom.[326] Some state laws require the collection of DNA from those suspected of unlawful presence.[327]

322. S.B. 1102, 52nd Leg., 1st Reg. Sess. (Okla. 2009) (named after Juli Busken, a University of Oklahoma student murdered in 1996). State lawmakers contend the expansion of DNA harvesting at the state level can bring "cold case" criminals to justice through "cold hit" DNA evidence. *See, e.g.*, Okla. State Senate Commc'n Div., *Gov. Signs Julie's* [sic] *Law* (May 20, 2009), http://www.oksenate.gov/news/press_releases/press_releases_2009/pr20090520g.html.

323. Persky, *supra* note 284, at 15 ("According to the National Conference of State Legislatures, all 50 states require that convicted sex offenders provide DNA samples. Increasingly, according to the conference, states are expanding these policies to include all felony convictions and even some misdemeanors as well.").

324. *See, e.g.*, OHIO JAIL ADMINISTRATORS, OHIO JAIL ADMINISTRATOR'S HANDBOOK 59 (2d ed. 2008), *available at* http://www.drc.state.oh.us/web/JailAdministratorHandbook.pdf; Zach Pluhacek, *State DNA Database To More Than Double Under New Law*, LINCOLN J. STAR ONLINE (Aug. 7, 2010, 12:55 AM) , http://journalstar.com/news/local/crime-and-courts/state-dna-database-to-more-than-double-under-new-law/article_a459b808-a1b4-11df-b90d-001cc4c03286.html.

325. Pluhacek, *supra* note 324.

326. *See, e.g.*, Tracey Maclin, *Is Obtaining an Arrestee's DNA a Valid Special Needs Search Under the Fourth Amendment? What Should (and Will) the Supreme Court Do?*, 34 J.L. Med. & Ethics 165, 167 (2006); S.B. 851, 53rd Leg., 1st Sess. (Okla. 2011); *see also* DNARESOURCE.COM, STATE DNA DATABASE LAWS QUALIFYING OFFENSES (2011), *available at* http://www.dnaresource.com/documents/statequalifyingoffenses2011.pdf.

327. S.B. 851, 53rd Leg., 1st Sess. (Okla. 2011) (permitting DNA collection from "any alien unlawfully present under federal immigration law").

According to the National Conference of State Legislatures, all fifty states and the District of Columbia require the collection of DNA samples from newborns for genetic screening purposes.[328]	Hospitals	DNA "stored in state labs for anywhere from three months to indefinitely, depending on the state."[329] In some states, genetic screening for diseases is conducted by taking blood samples of the newborn child without parental consent.[330]
"Bring Your Genes to Cal"	University of California, Berkeley	Since 2010, incoming freshmen at UC Berkeley can voluntarily submit to genetic testing.[331]

Table 12. Examples of Fingerprint Data Harvesting Programs

Program	Entity	Description
Secure Communities (S-COMM)	ICE/FBI[332]	Fingerprint-based arrest protocol requiring biometric database screening of anyone apprehended by state and local law enforcement through DHS and FBI databases.[333]
United States Visitor and Immigrant Status Indicator Technology	USCIS	Requires biometric data collection (fingerprint scans) of all noncitizen

328. *See Newborn Genetic and Metabolic Disease Screening*, NAT'L CONFERENCE OF STATE LEGISLATURES (Nov. 2007), http://www.ncsl.org/issues-research/health/newborn-genetic-and-metabolic-screening-laws.aspx.

329. Elizabeth Cohen, *The Government Has Your Baby's DNA*, CNN.COM (Feb. 4, 2010, 9:11 AM), http://www.cnn.com/2010/HEALTH/02/04/baby.dna.government/index.html.

330. *Id.*

331. Ferris Jabr, *California Legislators' Effort To Prevent Student DNA Testing Could Come Too Late: A New Bill Is Designed To Halt Berkeley's Controversial Genetic Testing Project*, SCIENTIFICAMERICAN.COM (July 9, 2010), http://www.scientificamerican.com/article.cfm?id=berkeley-bill-dna-testing.

332. All state and local law enforcement agencies are required to implement S-COMM by 2013 by DHS mandate. *See Secure Communities*, *supra* note 131. "As of August 22, 2012, the biometric information sharing capability [of S-COMM] is activated in 3,074 jurisdictions in 50 states, 4 territories and Washington D.C. During FY2013, ICE plans to use this capability nationwide." U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, ACTIVATED JURISDICTIONS (2012), *available at* https://www.ice.gov/doclib/secure-communities/pdf/sc-activated2.pdf.

333. *See Secure Communities*, *supra* note 131.

(US-VISIT), incorporating the National Security Entry-Exit Registration System (NSEERS)		visitors to the United States.[334]
Fingerprint Scanning Program at Walt Disney World	Walt Disney Corporation	"[V]isitors to Disney World must now provide a fingerprint in an effort to prevent sharing of tickets[.]"[335]
Thumbprint Signature Program[336]	Private banking institutions	Utilized by numerous state bankers associations, thumb scan may be required to open a bank account or to cash a check.[337]
CLEAR Pass or ClearMe.com	Private airport screening	"CLEAR automates the identity check process using biometrics, (fingerprints and iris)."[338]
MorphoTrak[339]	Private health clubs	Index fingerprint used for gym membership.[340]
Anti-Gang Neighborhood Protection Act of 2009 (California)[341]	Private gun dealers	Effective February 1, 2011, submission of fingerprints required to purchase ammunition in

334. *See Fact Sheet: US-VISIT Program*, *supra* note 312.

335. Cate, *supra* note 34, at 459 (footnote omitted).

336. *See e.g.*, *Thumbprint Signature Program*, IND. BANKERS ASS'N, http://www.indianabankers.org/displaycommon.cfm?an=1&subarticlenbr=16#.T1OKZvGPWf4; *Thumbprint Signature Program—Check Fraud Deterrent*, N.Y. BANKERS ASS'N, http://www.nyba.com/profitsolutions/thumbprint-signature-program-check-fraud-deterrent/.

337. *See* Pascal Fletcher, *No Thumbprint, No Money, Bank Tells Armless Man*, REUTERS (Sept. 3, 2009, 10:51 AM), http://www.reuters.com/article/2009/09/03/us-bank-thumbprint-idUSTRE58247Y20090903.

338. *Home*, CLEAR, http://clearme.com. CLEAR's website provides a brief explanation of how expedited airport screening is conducted by the private corporation, including background check that requires collection of biometric data (fingerprints and iris scans). *See CLEAR FAQs*, CLEAR, http://clearme.com/faqs. This service is offered at Denver International Airport (DEN), Orlando International Airport (MCO), San Francisco International Airport (SFO), Dallas/Ft Worth International Airport (DFW), and Westchester NY Airport (HPN). *Id.*

339. 24-Hour Fitness utilizes MorphoTrak, a biometric scanning technology, and adopted a test pilot program in sixty gyms in California in August 2010. Demian Bulwa, *Fingerprint Check-in Tried at 24 Hour Fitness*, SFGATE.COM (Aug. 23, 2010, 4:00 AM), http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/08/23/MN201EVV36.DTL.

340. *Id.*

341. Assemb. B. 962, Ch. 628, 2009-2010 Gen. Assemb., Reg. Sess. (Cal. 2009).

		California. Requires that all ammunition sales in California involve a face-to-face transaction and fingerprint registration of the purchasers. Use of online sites or catalogues requires ammunition shipped to a local gun dealer: transaction must be performed in person under the law.[342]

Table 13. Examples of Facial Recognition Data Harvesting Programs

Program	Entity	Description
REAL ID Act of 2005 & Driver's License Facial Recognition Application	DHS	At least thirty-four states use facial recognition systems to "verify a person's claimed identity and track down people who have multiple licenses under different aliases."[343]
U.S. Passports and e-Passports	DoS	Passports and e-Passports require digital photo that is provided to centralized facial recognition database.[344]
E-Verify Photo Tool[345] (incorporated into E-Verify in 2007)[346]	USCIS/SSA	Allows employers to match the photo on an employee's EAD

342. Fresno County Superior Court Judge Jeffrey Hamilton ruled the law unconstitutional in January 2011. Parker v. California, No. 10 CECG 02116 (Cal. Super. Ct. Jan. 31, 2011).

343. Meghan E. Irons, *Caught in a Dragnet*, BOS. GLOBE (July 17, 2011), http://www.boston.com/news/local/massachusetts/articles/2011/07/17/man_sues_registry_after_license_mistakenly_revoked/?page=full. Although REAL ID does not require facial recognition technology, the statute is the impetus behind state adoption of this technology. JANICE KEPHART, CTR. FOR IMMIGRATION STUDIES, REAL ID IMPLEMENTATION ANNUAL REPORT: MAJOR PROGRESS MADE IN SECURING DRIVER'S LICENSE ISSUANCE AGAINST IDENTITY THEFT AND FRAUD (2012), *available at* http://www.cis.org/sites/cis.org/files/articles/2012/real-id-2012.pdf.

344. *The U.S. Electronic Passport*, *supra* note 183.

345. *See* GAO EMPLOYMENT VERIFICATION, *supra* note 109, at 11 ("For noncitizens who show a Permanent Resident ('green') card or employment authorization document as proof of identity and employment eligibility, the system is to transmit a digitally stored photograph of the employee to the employer. It is the employer's responsibility to determine whether the

		[Employment Authorization Document] or a Permanent Residence Card ("green card") to the photo that USCIS has on file for that employee.[347]
Scotland Yard's identification of rioters after 2011 London riots	Scotland Yard via Facebook & Twitter	Surveillance technology (CCTV) interfaces facial recognition software with social media sites (Facebook and Twitter) to identify rioters.[348]

B. Identity Verification Through Biometric Data Matching

Once biometric data has been harvested, it must be compiled within a database, which in turn makes possible identity screening: the verification of a person's identity by matching him or her with the data concerning that person in the database. Although an oversimplification, the use of biometric data in identity verification can be described as a four-step process: Enrollment, Capture, Comparison, and Decision.[349] Each step is briefly summarized as follows. (1) *Enrollment*: An individual first identifies himself and actually puts his fingerprint down, has a digital photo taken, has eyes scanned, etc. (2) *Capture for Recognition*: A template for that identity is created to use for future identification purposes. (3)

---

photograph provided by the employee matches the electronic photograph provided by E-Verify." (footnote omitted)).

346. *Id.* at 22 ("USCIS has taken actions to address fraud, most notably with the fiscal year 2007 implementation of the photo matching tool, which seeks to reduce fraud associated with the use of genuine documents in which the original photograph is substituted for another.").

347. *Id.*

348. *See UK Using Facial Recognition To Hunt Rioters*, CBSNEWS.COM (Aug. 11, 2011, 10:55 AM), http://www.cbsnews.com/2100-202_162-20091186.html.

349. *See, e.g.*, VACCA, *supra* note 3, at 23–27; BIOMETRIC RECOGNITION, *supra* note 3, at 25–26. For clarification, not all protocols involve all four steps. However, any given protocol could involve the four-step process during any given encounter, depending on what is being asked of the data collector and data screener. Also, I note that Vacca identifies a three-part procedure: "Enrollment," "Verification" ("Comparison"), and "Identification" ("Decision"). VACCA, *supra* note 3, at 23–27. For the purposes of further clarification, I have described the Enrollment process as a four-part procedure, breaking the Enrollment procedure down into two separate parts: "Enrollment" and "Capture for Recognition." Other experts have described the biometric data enrollment and recognition process as a five-part procedure: "Enrollment and Recognition Phases," "Sensor [M]odule" (selecting appropriate sensor or biometric reader for biometric data "Capture"), "Feature [E]xtraction [M]odule" (process of biometric data "Capture"), "Database [M]odule" ("Comparison"), and "Matching [M]odule" ("Decision"). *See* JAIN ET AL., *supra* note 3, at 4–10. For ease of description, I have included the process of sensor module selection as a part of the Enrollment process.

Comparison: The individual's currently presented biometric data (e.g., fingerprint or iris scan) is cross-referenced with the originally presented biometric data (e.g., enrollment and identity template). And (4) *Decision*: Statistical algorithms are developed to "match" the probability that the initial biometric data can be accurately compared to the currently presented biometric data or to make a determination that the data does not "match."

As a brief overview, it is significant to observe that the utilization of biometric data for mass identification on a scale of 300 million individuals or more—the population of the United States—is considered highly experimental.[350] The development of automated biometric ID data matching systems through digitalized credentialing is both experimental technologically and policy-wise. Based on recent comprehensive immigration reform bills and other immigration legislation, however, it appears this experimental technology and policy prescription has been growing steadily in acceptance over the past decade.

Yet, many experts have concluded that biometric data is an unstable and unreliable foundation for verifying identity on an automated mass scale of hundreds of millions of individuals.[351] The reason is relatively straightforward. Unlike other identity verification protocols where there is a 100% accuracy match rate in the decision (e.g., through 100% match of a PIN number or 100% match of an identity security token), in biometric identity verification, 100% accuracy is a 100% technological impossibility. In fact, 100% accuracy in biometric identity verification is a sign of fraud.[352] Consequently, at any level below 100% accuracy, identity verification in biometric technology necessitates an ironic conclusion: you may not be able to confirm your identity because of inaccuracies in the data or because of other technological limitations.

Accepting false positives and false negatives, therefore, are the necessary preconditions for adopting biometric identity verification technology. For example, if, on a scale of one to one hundred, seventy is deemed as the minimum score needed for a match, there will be some individuals scoring below seventy that have given genuine fingerprints. Likewise, there will be some individuals scoring above seventy that have given fraudulent fingerprints. The higher the minimum score, the less often fraudulent fingerprints are returned as a match, but the more often genuine fingerprints may be rejected. Who decides what accuracy level is appropriate for the purposes at hand and how that accuracy rate is assessed becomes critically important. Currently, the federal government outsources the

---

350. *See, e.g.*, GATES, *supra* note 3, at 5 (explaining the experimental nature of biometric ID technologies); MAGNET, *supra* note 3, at 3–16, 30–31; GAO TECHNOLOGY ASSESSMENT, *supra* note 3, at 136–221 (describing the projected maturation process of the testing and implementation of various biometric identification technologies).

351. *See, e.g.*, BIOMETRIC RECOGNITION, *supra* note 3, at viii–ix (discussing experimental nature of biometric recognition and matching technologies).

352. *See id.* at 4–5, 12 ("A biometric match represents not certain recognition but a probability of correct recognition [based on statistical algorithms that match biometric data captured with biometric databases.]"). Because biometric identity verification matching depends on probabilistic matching, the determination is always less than 100%. *See id.* Therefore, the only way one could reach a 100% match through biometric verification matching is through tampering or other system compromise. *See id.*

management of its biometric identification technologies to private corporate "vendors."[353] Vendors are not required to test for accuracy and also are not required to provide results of "no-matches," or how a "match" or "no-match" is decided, to the government.[354] There is no regulatory body of the federal government that oversees what biometric data standards or technologies are considered minimally proficient.[355]

Moreover, utilizing a digitalized biometric ID or biometric database screening technology removes the matching process from the trained expertise of specific forensic experts and places the matching process into an automated system. The accuracy of the automated biometric data matching process, therefore, is driven by the capabilities and limitations of the software (e.g., the statistical algorithms) and the hardware (e.g., the scanning technology that collects the data and the sorting technology that analyzes the data). The accuracy of the assessment also depends upon the technological proficiencies of those tasked with enrolling the initial biometric data (e.g., establishing the initial biometric data template) and the capture of future biometric data (e.g., law enforcement or immigration agents seeking biometric data through portable, handheld biometric screeners (or mobile biometric sensors) to compare captured biometric data with the government's biometric databases).

In short, both the underlying databases and the database screening technology, and the attendant scientific and programmatic safeguards required to regulate the databases and technology, have been unable to keep up with the burdens increasingly placed on such systems.[356] Nevertheless, multiple statutes and the programs they authorize advanced since the 9/11 terrorist attacks demonstrate that database screening technologies and biometric data, in particular, are increasingly

---

353. *Id.* at 8 (describing the difficulty of assessing the capability of a potential vendor's technology).

354. Because these technologies are emerging and experimental, they have not been thoroughly peer reviewed. *See, e.g.*, GARFINKEL, *supra* note 3, at 59 ("It's important to realize that *none* of the [biometric] techniques mentioned here have gone through the kind of thorough peer review that was required of DNA fingerprinting in the 1980s and early 1990s." (emphasis in original)). Private biotech corporations, also referred to as vendors, largely control the testing of biometric verification technologies. *See, e.g.*, GAO TECHNOLOGY ASSESSMENT, *supra* note 3, at 58 ("Biometric companies have primarily been concerned with testing the accuracy of their technologies in highly controlled environments, using static or artificially generated templates, images, and data. The results of their tests, as quoted by vendors, are quite extraordinary . . . because the performance of a technology depends greatly on how and where it is deployed, such numbers have proven to be far more impressive than real-life performance data.").

355. Currently, NIST is tasked with overseeing testing of biometric technologies by the federal government but does not set minimally proficient standards. *See* GAO TECHNOLOGY ASSESSMENT, *supra* note 3, at 54 ("Biometric technologies are maturing but are still not widespread or pervasive because of performance issues, including accuracy, the lack of applications-dependent evaluations, their potential susceptibility to deception, the lack of standards, and questions of users' acceptance.").

356. *See, e.g.*, SOC. SEC. ADMIN. OFFICE OF THE INSPECTOR GEN., CONGRESSIONAL RESPONSE REPORT: ACCURACY OF THE SOCIAL SECURITY ADMINISTRATION'S NUMIDENT FILE (2006), *available at* http://oig.ssa.gov/sites/default/files/audit/full/pdf/A-08-06-26100.pdf.

viewed by policymakers as a zero-risk tolerance solution to the problem of identity verification in order to secure the border.[357]

C. Limitations of Biometric Data Matching and Biometric ID Technologies

Biometric database screening is increasingly viewed by some key policymakers as the "gold standard" by which to accurately verify identity and citizenship status.[358] In the context of homeland security policy and immigration control, therefore, biometric technology is increasingly considered by the political branches as an efficacious solution because it adopts the "gold standard" of identification for identity management systems.[359] Consequently, it is characterized in policy proposals as one of the most effective methods by which to prescreen individuals before the grant of certain rights and privileges. As discussed above, identity management tools and systems attempt to verify identity before authorizing the right to work (e.g., E-Verify),[360] the right to drive (e.g., REAL ID driver's licenses),[361] the right to vote (e.g., Help America Vote Act),[362] in order to more effectively secure the border and screen out the potential terrorist and criminal alien or unlawfully present immigrant. Yet, biometric technologies are not without problems and limits.

Many experts have concluded that the technology and processes required to safely and accurately conduct the automated biometric matching of hundreds of millions of individuals on a national scale simply do not exist.[363]As explained in *Biometric Recognition: Challenges and Opportunities*, a report published by the National Academies Press, edited by Joseph N. Pato and Lynette I. Millet, a science fiction understanding of biometric data screening and sorting technology often governs debates about the efficacy of such technology.[364] Popular misconceptions

---

357. *See, e.g.*, FROOMKIN & WEINBERG, *supra* note 3.

358. *See* Alan Gomez, *Immigrant Tracking May Impede Bill; Partisan Split Developing over Biometric Data on Foreigners Leaving U.S.*, USA TODAY, May 9, 2013, at A5 ("[Former U.S. Secretary of Homeland Security Michael] Chertoff calls [biometrics] the 'gold standard.'").

359. *See supra* notes 2, 4, 39, and accompanying text.

360. E-Verify as of yet does not require a biometric data identifier. However, congressional proposals surrounding the extension of the E-Verify program have discussed adding a biometric verification component. *See supra* notes 37, 238, and accompanying text (discussing BELIEVE).

361. Similarly, although the REAL ID Act of 2005 does not require the biometric verification of a fingerprint, REAL ID does include technological enhancements and requires digital photos that can be analyzed with facial recognition software. *See* REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 302 (codified as amended in scattered sections of 8 U.S.C.).

362. Help America Vote Act of 2002 (HAVA), which relies upon SSA database screening of Social Security Numbers, does not yet require a biometric data matching component. 42 U.S.C. § 15483(a) (2006) (implementing provision); GAO EMPLOYMENT VERIFICATION, *supra* note 109; REAL ID Act of 2005, Pub. L. No. 109-13, § 202(b)–(d), 119 Stat. 302, 312–14 (implementing provisions).

363. *See, e.g.*, BIOMETRIC RECOGNITION, *supra* note 3, at vi–ix.

364. *Id.*

regarding the capabilities of biometric identification have been entrenched through cultural influences, such as science fiction and futuristic films.[365] These cultural biases complicate an ability to grasp the distinction between the efficacy of individualized biometric matching based on case-by-case determinations that utilize the training and judgment of human experts (e.g., a forensics expert at a crime scene), on the one hand, and mass biometric matching of millions of individuals based on large-scale, digitally generated determinations, on the other hand.[366]

Another risk arising from the removal of the biometric data matching process from a specific and narrowly tailored context (such as a prosecutorial context for the purposes of establishing evidence for specific crimes) to a universal and general-purpose context (such as identity and citizenship status verification) is that it significantly increases the potential for the future abuse of biometric data. The potential misuse or unlawful treatment of such data matching or data screening protocols by both the public and private sectors is expanded, therefore. Genetic ethicists note that attempts by scientists to decode DNA in recent decades, for example, have led to classifications that draw correlative evidence between genetic markers that signify race, ethnicity, religion, etc., and behavioral analytics such as criminal disposition, intelligence testing, etc.[367] The private health information that could be yielded through a universal DNA database would require a reconceptualization of what medical privacy could be protected once such a database exists.[368] Therefore, experts predict that a universal DNA database poses risks of demographic and behavioral profiling, as well as health and medical profiling, in ways that may be challenging or impossible to regulate or mitigate.[369] Further, the premature adoption of a biometric-based identification system on a mass scale is advised against in part because of the severe restrictions on an individual's ability to exercise due process rights.[370] For example, such a system would likely neither allow for an interrogation of the "chain of evidence" nor afford a process for confronting the databases or algorithms from which the conclusions are drawn, let alone the individuals charged with implementing the screening.[371]

Many identity management programs already in place demonstrate programmatic challenges that can stem from the lack of expertise of those tasked with the collection of the personally identifiable data and conducting the database screening. DHS, for example, delegates implementation of the E-Verify program to

---

365. *Id.*

366. *Id.*

367. *See, e.g.*, DUSTER, *supra* note 263. For an excellent discussion on how developments in neuroscience pose similar challenges to the Fourth and Fifth Amendments, see respectively Farahany, *Searching Secrets*, *supra* note 6; Farahany, *Incriminating Thoughts*, *supra* note 6.

368. *See generally* DUSTER, *supra* note 263 (describing the implications for racial profiling of a national DNA database in criminal law).

369. *See, e.g.*, EUGENE THACKER, THE GLOBAL GENOME: BIOTECHNOLOGY, POLITICS, AND CULTURE (2005).

370. BIOMETRIC RECOGNITION, *supra* note 3, at 10–11.

371. *See generally* Jennifer L. Mnookin, *The Courts, the NAS, and the Future of Forensic Science*, 75 BROOK. L. REV. 1209 (2010); Roth, *supra* note 29.

employers, who agree to screen new hires through DHS and SSA databases.[372] DHS also delegates implementation of the S-COMM program to state law enforcement officials, who agree to collect and screen the biometric data (e.g., fingerprints) of arrestees through DHS and FBI databases.[373] Those screened face potential legal and other consequences depending on the results of the experimental database screening. Thus, serious questions remain as to whether such digital data collection and database-screening protocols are appropriately delegated to state and private actors for federal identity verification purposes. A separate question remains as to whether these actors should be empowered to impose, in a de facto manner, downstream consequences,[374] such as the denial of employment opportunities and deportation proceedings, through database screening, especially if such actors fail to properly collect and screen the data pursuant to the federal government's guidelines.

In addition, to ground concretely the limitations of such technology, it is instructive to examine the challenges faced by the government in the implementation of a government-wide digitalized biometric ID program. The National Institute of Standards and Technology (NIST) as well as other scientists and experts have identified a variety of concerns surrounding biometric ID data as a primary data point for identification.[375] These concerns include liveness detection, revocability, reliability, and security.

1. Liveness Detection

Studies on biometric identification technologies have indicated that biometric fraud is possible due to technological limitations in detecting biometric "liveness." In other words, how does the system recognize whether the fingerprint that is being scanned digitally has been stolen and has been replicated? For example, how does the scanner detect whether it is digitally scanning latex gloves or silicone-sculpted fingerprint tips? How does any system administrator ensure that the individual using the system is using a live fingerprint? The biotech industry has not yet developed the technology yet to ensure the fingerprint is not forged. Even if a system administrator is watching an individual provide a fingerprint, they may not be able to tell whether the fingerprint is "live" or forged. Research done in this area is sparse, and, currently, no verifiable standards exist.[376]

---

372. *See generally* GAO EMPLOYMENT VERIFICATION, *supra* note 109.

373. *See Secure Communities*, *supra* note 131.

374. Stephen Lee, *De Facto Immigration Courts*, 101 CALIF. L. REV. (forthcoming 2013) (exploring the manner in which state criminal courts and prosecutors are seizing the reins of federal policymaking discretion through state and local immigration screening and exercise of prosecutorial discretion, resulting in downstream consequences, such as deportation).

375. *See, e.g.*, BIOMETRIC RECOGNITION, *supra* note 3, at viii–ix (discussing experimental nature of biometric matching technologies); WILLIAM MACGREGOR, KETAN MEHTA, DAVID COOPER & KAREN SCARFONE, NAT'L INST. OF STANDARDS & TECHS., A RECOMMENDATION FOR THE USE OF PIV CREDENTIALS IN PHYSICAL ACCESS CONTROL SYSTEMS (PACS), 12–15 (2008) (describing some "known technical threats" to PIV system); MAGNET, *supra* note 3, at 3–16, 30–31.

376. *See* MAGNET, *supra* note 3, at 27 (citing various studies verifying methods for

2. Revocability

Currently, there is no remedy available if an individual's biometric data is stolen. Technologically, there is no way to develop encryptions within our biometric data because our biometric data is derived from our body. For instance, if someone steals biometric information that is embedded in a microchip on a gym card or bank card, this biometric information can be used to perpetrate the acquisition of a fraudulent biometric-based REAL ID driver's license. NIST also notes that there is no research on how robust fingerprint data is over time or how data captured on one type of machine would be translated once newer technology is used to replace older hardware or obsolete software.[377]

3. Reliability

In biometric-verification technology, accuracy improves if all other factors remain stable in the environment. For example, NIST has learned through PIV card/biometric ID card implementation that the same vendor should be used to ensure higher accuracy.[378] Biometric technology users are instructed to attempt to ensure that the environment for the biometric data enrollment and the verification are identical (e.g., attempt to use same staff, same room, same lighting, and same humidity levels).[379] In addition, experts have realized that biometric verification systems need to develop an alternative system for people with no fingerprints, those with "damaged" fingerprints, dysplasia resulting in no lines in fingerprints, and so forth.[380] Biometric research has determined that biometric data is less accurate and harder to recognize for women (fine skin and less defined fingerprints due to housecleaning solution and face cleansing) and the elderly (loss of collagen).[381]

---

successfully circumventing biometric technology, including artificial gelatin imprints).

377. JAIN ET AL., *supra* note 3, at 37.

378. Due to these concerns, the NIST began a program for evaluating and setting standards for vendor interoperability, called MINEX. *See generally MINEX Overview*, NAT'L INST. OF STANDARDS & TECHS. (OCT. 27, 2011), http://www.nist.gov/itl/iad/ig/minex.cfm.

379. *See, e.g.*, BIOMETRIC RECOGNITION, *supra* note 3, at 8 ("Achieving automated recognition involves the proper functioning of a broader system with many elements, including the human sources of data, human operators of the system, the collection environment(s), biometric sensors, the quality of the system's various technological components, the human-sensor-environment interaction, biometric reference information databases and the quality and integrity of the data therein . . . .").

380. *See* SAMIR NANAVATI, MICHAEL THIEME, RAJ NANAVATI, BIOMETRICS: IDENTITY VERIFICATION IN A NETWORKED WORLD 59–60 (2002) ("Certain ethnic and demographic groups have lower-quality fingerprints and are more difficult to enroll than others. IBG's Comparative Biometric Testing has shown that elderly populations, manual laborers, and some Asian populations are more likely to be unable to enroll in some finger-scan systems.").

381. *See The Real World Is Diverse*, LUMIDIGM, http://www.lumidigm.com/population-characteristics/ ("Age is another physiological characteristic that can affect the ability of a [biometric] sensor to collect a usable fingerprint image. One effect of aging is the loss of collagen in the skin; elderly fingers have soft fingerprint ridges that collapse into each other when the finger touches a surface. Because many sensor technologies depend on the quality

Biometric research has also determined that the statistical algorithms have a racially disparate impact in accuracy for reasons that are not fully understood.[382] Finally, biometric technology has not yet adopted a uniform standard domestically or internationally. Some advocate adoption of the INTERPOL fingerprinting standard, which is similar to the American standard (e.g., using image and points within fingerprint). This matter, however, remains unresolved.[383]

4. Security

As discussed above, many experts have concluded that the technology does not currently exist to support a reliable biometric ID data matching system on a national, mass scale. Such a system would require the accurate and secure capture, storage, data use, and analysis of the biometric data of hundreds of millions of citizens and noncitizens.[384] Research is still needed to develop an accurate scientific foundation to support mass biometric matching systems.[385] Additionally, experts note the inability to safeguard biometric data because, for example, we leave our fingerprints and DNA traces everywhere we go.[386] Therefore, it is difficult to protect biometric data from nonconsensual data capture and database screening,[387] and identity theft vulnerabilities.[388] Because biometric data cannot be safeguarded, it is among the least secure forms of personally identifiable data. As one security expert explained it succinctly: "[B]iometrics are easy to steal. . . . Biometrics are unique identifiers, but they're not secrets."[389] Yet, as also observed above, other experts note that the new post-9/11 national security paradigm of zero-risk tolerance applies pressure on policymakers to develop solutions that reduce the statistical risk of terrorist attack, even as experts note that the real risk of terrorism cannot be reduced.[390] Thus, it should be noted that some experts contend a

---

of contact between the finger and the sensor to collect a good image, soft fingerprint ridges can be difficult to image."); *see also* MAGNET, *supra* note 3, at 30.

382. *See, e.g.*, MAGNET, *supra* note 3, at 28–29.

383. *See* VACCA, *supra* note 3, at 65 (describing ongoing attempts to create generic international biometric standards).

384. *See, e.g.*, BIOMETRIC RECOGNITION, *supra* note 3, at 5 ("Even very small probabilities of misrecognitions—the failure to recognize an enrolled individual or the recognition of one individual as another—can become operationally significant when an application is scaled to handle millions of recognition attempts.").

385. *Id.* at 13 ("[A] scientific basis is needed for the distinctiveness and stability of various biometric traits under a variety of collection processes and environments and across a wide population over decades.").

386. *See, e.g.*, Schneier, *supra* note 5.

387. *See, e.g.*, Farahany, *Searching Secrets*, *supra* note 6, at 1281 ("Should the motorist refuse to provide her identity, the police might nevertheless employ biometric technology to quickly and unobtrusively identify her.").

388. *See, e.g.*, Joh, *supra* note 6.

389. Schneier, *supra* note 5.

390. *See, e.g.*, BRIAN MICHAEL JENKINS, UNCONQUERABLE NATION: KNOWING OUR ENEMY, STRENGTHENING OURSELVES 152–54 (2006).

biometric national ID card will not increase security and, in fact, could increase national security risks.[391]

IV. OVERVIEW OF BUREAUCRATIZED CYBERSURVEILLANCE

More and more policy experts are calling for multimodal biometric identification systems—for instance, which combine facial recognition, fingerprints, iris scans, and/or DNA—to increase the reliability of identity screening systems.[392] Yet, the surveillance consequences of such programs and protocols are obscured because they are implemented in a manner that may appear to be reasonable (e.g., ID cards)[393] and expected (e.g., identity or citizenship status verification protocols).[394] Additionally, the surveillance consequences are also obscured because these methodologies may appear on their face to be consensual (e.g., voluntarily submitting to Internet database-screening protocols which, in turn,

---

391. *See, e.g.*, Bruce Schneier, *A National ID Card Wouldn't Make Us Safer*, SCHNEIER ON SEC. (Apr. 1, 2004), http://www.schneier.com/essay-034.html; Jim Harper, *Rejecting National ID*, AMERICAN SPECTATOR (Feb. 7, 2008, 12:06 AM), http://spectator.org/archives/2008/02/07/rejecting-national-id. *But see The Case for a National ID Card*, WASH. POST OPINIONS (Feb. 2, 2013), http://articles.washingtonpost.com/2013-02-02/opinions/36701587_1_illegal-immigrants-immigration-reform-immigration-system.

392. *See, e.g.*, Donohue, *supra* note 3, at 442 (explaining FBI's expansion of biometric data collection under NGI: "The solution was to move beyond a unimodal biometric identifier (e.g., fingerprints), and towards multimodal biometric identifiers, such as FRT [facial recognition technology], and voice, iris recognition technologies."); LYNCH, *supra* note 3, at 10 ("Traditionally, biometrics databases such as IAFIS and IDENT have collected only one biometric at a time. However, the government has argued these 'unimodal' systems are limited and has been pushing to develop 'multimodal' systems that collect and combine two or more biometrics (for example, photographs and fingerprints). The government argues that collecting multiple biometrics from each subject will make identification systems more accurate." (footnote omitted)); GAO TECHNOLOGY ASSESSMENT, *supra* note 3; Kephart, *supra* note 260; *Measuring the Outcomes*, *supra* note 260; Wilson, *supra* note 260.

393. In deciding to relinquish privacy rights, some scholars have observed that what appears to be reasonable cognitively is transforming in the realm of modern society and cyberspace transactions in particular. *See, e.g.*, SOLOVE, *supra* note 10; Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998). Some scholars attribute this to an asymmetrical information problem. *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056 (2004). Examining privacy torts or privacy expectations in privacy law can be instructive in light of the challenges of modern technology and data breaches. *See, e.g.*, Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010).

394. Reasonable expectations of privacy are notoriously difficult to define, especially in the data privacy context. *See, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1397 (2000); Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 MINN. L. REV. 1588 (2010); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727 (1993).

permits the harvesting, aggregation, and analysis of identity data).[395] Further, the manner in which personally identifiable data is shared by the citizen with the government or other third parties may not appear to implicate traditional privacy concerns (e.g., employer identity database screening of employees as directed by law as a precondition for hiring).[396] One of the hallmarks of cutting-edge cybersurveillance is that it can also be conducted remotely and automatically,[397] virtually and near invisibly,[398] constantly and near costlessly.[399]

A. Bureaucratized Cybersurveillance Programs and Dataveillance Protocols

The process of surveillance normalization that now appears to be unfolding tracks a transition from an era of traditional bureaucratized surveillance to an era of bureaucratized cybersurveillance. Identity verification programs and protocols—including programs which incorporate immigration status screening and citizenship status checks—can be executed through traditional bureaucratized surveillance (e.g., physical document inspection) or through bureaucratized cybersurveillance (e.g., collection of personally identifiable data and database screening). Identity verification screening protocols have traditionally entailed the request for the production of identity and immigration or travel documents. During the course of the inspection, the inspector confirms the document is valid, unexpired, and relates

---

395. Many scholars have theorized the profound social and legal impact of technological innovation and the Internet in particular on society and a digital civilization. *See, e.g.*, LESSIG, *supra* note 8; MARK POSTER, INFORMATION PLEASE: CULTURE AND POLITICS IN THE AGE OF DIGITAL MACHINES (2006); JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000).

396. The law of information privacy has been described by scholars as "increasingly fragmented and decreasingly coherent." Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007, 2007 (2010). Even when privacy is intended to be protected, some scholars have noted the manner in which this protection fails in the cyberprivacy context. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); *see also* Chamber of Commerce v. Whiting, 131 S. Ct. 1968 (2011) (upholding Legal Arizona Workers Act of 2007 which makes E-Verify Internet database screening mandatory for all Arizona employers); NASA v. Nelson, 131 S. Ct. 746 (2011) (upholding background check procedure in HSPD-12 as not violating right to informational privacy).

397. The automatic disclosure of information to automated third parties and automated decision making by agencies both present novel constitutional concerns. *See, e.g.*, Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581 (2011).

398. *See, e.g.*, SLOBOGIN, PRIVACY AT RISK, *supra* note 21. For post-9/11 developments in surveillance and dataveillance technology, see O'HARROW, *supra* note 3; PRIEST & ARKIN, *supra* note 13.

399. Data-driven cybersurveillance and dataveillance impose minimal costs on persons collecting the data transmittal of the digital data, as compared with traditional forms of surveillance (e.g., assigning an agent to physically follow a suspect). Although the collection and transmittal of data may not be as costly, cybersurveillance and dataveillance methods are not cost free. The maintenance, aggregation, and analysis of databases can entail tremendous expense.

to the person producing the ID. Increasingly, however, identity verification protocols utilize both the physical inspection of identity documents, as well as Internet-driven or digitalized data-driven screening through public and private databases. Policymakers are increasingly calling for the implementation of a digitalized national ID system to facilitate universal data collection and database screening to verify identity.[400]

Tables 14 and 15 show how traditional forms of bureaucratized surveillance are transforming in light of emerging cybersurveillance and dataveillance technologies and programs. Table 14 focuses on the broad categories of traditional bureaucratized surveillance. Table 15 focuses on how bureaucratized cybersurveillance is adding an entirely new cybersurveillance and dataveillance dimension to the protocols of traditional bureaucratized surveillance.

Table 14. Examples of Bureaucratized Surveillance v. Bureaucratized Cybersurveillance

Category	Traditional Bureaucratized Surveillance	Bureaucratized Cybersurveillance
Identity Cards	Passport; driver's license; Social Security Card; etc.	e-Passports; RFID-enhanced passports and other digitalized IDs; REAL ID Act driver's licenses and RFID-enhanced driver's licenses; RFID-enabled smart cards; GPS-enabled smartphones as form of digitalized ID; proposals for "high-tech" Social Security Card; etc.
Identity Registration	Alien registration protocols; requirements to carry identity papers on the body; paper files and dossiers; nondigitalized databases; etc.	Automated and invisible geolocational, biometric, behavioral, and biographical data tracking; digital dossiers; merger of public and private sector databases
Population Statistics	Census statistics; population mapping; etc.	Group-based and pattern-based data aggregators and data refineries; data-driven methods to track behaviors of population and sub-populations
Identity Verification	Document production and inspection procedures (e.g., "Show Me Your Papers" protocols)	Delegation of data collection and database screening to private sector and states; remote and automatic data collection and screening; data

400. *See, e.g.*, Yadron, *supra* note 239; *see also* Jim Harper, *Internal Enforcement, E-Verify, and the Road to a National ID*, 32 CATO J. 125, 130 (2012).

		mining and data matching; data aggregation; database screening, including Internet-based screening; algorithms attempting to authenticate identity and attempting to predict or analyze biographical and behavioral data

Table 15. Examples of Emerging Protocols Under Bureaucratized Cybersurveillance

Protocol	Traditional Bureaucratized Surveillance	Bureaucratized Cybersurveillance
Border Crossing and Border Security	Physical document inspection of passport, visa, etc.	e-Passport, RFID-enhanced passports and other digitalized IDs; US-VISIT (digitalized collection and screening of biometric data of all noncitizens visiting the United States); BCC (digitalized biometric-based border crossing card); database screening through TECS, ATS, TIDE, SEVIS, etc.; America's Shield Initiative (ASI) and Integrated Surveillance Intelligence System (ISIS); drones; search and seizure of information technologies (laptops, mobiles, and smartphones)
Airport Screening	Physical document inspection of driver's license, physical screenings, etc.	CLEAR Pass or ClearMe.com (digitalized collection of biometric data to expedite traveler screening); Global Online Enrollment System (GOES) or Global Entry Trusted Traveler System; Secure Flight and "No-Fly List" (database screening and aggregation of multiple databases to predict threat risk); body scanners
Employment	Physical document	Social Security Number

Eligibility Screening[401]	inspection of Social Security Card, driver's license, etc., pursuant to Form I-9 (employment eligibility verification process)	screening and database screening of other personally identifiable data (e.g., Social Security Number Verification System (SSNVS) and E-Verify database screening as required under state immigration laws); E-Verify Photo Tool (digitalized photo databases); Social Security Number "DHS No-Match Rule" (rescinded)
Voter ID Laws[402]	Physical document inspection	Social Security Number screening and database screening of other personally identifiable data (HAVA database matching)
"Stop and Identify" Laws[403]	Physical document inspection of driver's license and identity documents	Department of Motor Vehicles database screening; potential use of social network screening technologies (e.g., Lighthouse) and biometric data screening (e.g., MORIS, HIIDE)
"Show Me Your Papers" Laws[404]	Physical document inspection of identity and immigration documents	Biometric data screening (fingerprint scans) under Section 1373(c) of the INA and S-COMM (digitalized collection of biometric data to facilitate immigration and criminal records screening); National Crime Information Center (NCIC) and other databases

401. *See, e.g.*, Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, § 101, 100 Stat. 3359, 3360 (1986) (codified as amended at 8 U.S.C. § 1324a); Hu, *supra* note 13, at 564–65, 579–86; Lee, *supra* note 13, at 1110–33.

402. *See, e.g.*, Atiba R. Ellis, *The Cost of the Vote: Poll Taxes, Voter Identification Laws, and the Price of Democracy*, 86 DENV. U. L. REV. 1023, 1034 (2009) ("[M]odern voter identification laws–specifically, those voter identification laws that require the presentation of a government-issued photographic identification card–focus most clearly on [a] proof-of-identity requirement. The key issue for these laws is what forms of information the voter must gather to prove his or her identity when registering and when appearing to vote.").

403. Michael S. Pardo, *Disentangling the Fourth Amendment and the Self-Incrimination Clause*, 90 IOWA L. REV. 1857, 1891–97 (2005) (discussing state "stop and identify" laws and the constitutionality of such laws under the Court's decision in Hiibel v. Sixth Judicial District Court of Nevada, 542 U.S. 177 (2004)).

404. *See* Hu, *supra* note 13 (discussing document-based and database-based screening protocols required under federal and state immigration screening).

Background Check	Screening through data files (e.g., criminal records, credit reporting, etc.)	Biometric data screening (digitalized collection and screening of biometric data); behavioral and moral character screening through social media trawling (Facebook, Twitter, Google, etc.); data mining (Acxiom, LexisNexis, etc.); aggregating contextual information; etc.

B. Rapid Expansion of Post-9/11 Identity Management and Biometric Dataveillance Programs

The identity management phenomenon is rapidly proliferating in the post-9/11 context. The phenomenon is difficult to examine and interrogate given the nature of cybersurveillance and that it is proliferating in a highly bureaucratized context, for example, through statutory and regulatory frameworks, and executive orders and presidential directives. Moreover, both the administrative and technological structures that support it are of an unusually complex and technical nature.

Table 16 provides examples of some of the identity management programs that have been promulgated since 9/11. This table primarily focuses on identity verification programs and does not include identity determination or identity inference programs, most of which are advanced and implemented through executive policies and administrative action.

Table 16. Examples of Post-9/11 Statutes Creating Identity Management Programs

Statute	Entity	Program
Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT Act of 2001)[405]	DHS	United States Visitor and Immigrant Status Indicator Technology (US-VISIT), incorporating the National Security Entry-Exit Registration System (NSEERS). Section 403(c) mandates the development of "a technology standard that can be used to verify the identity of persons applying for" or seeking entry into the U.S. on a visa "for the purposes of conducting background

405. Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered sections of the U.S.C.).

		checks, confirming identity, and ensuring that a person has not received a visa under a different name."[406]
Aviation and Transportation Security Act [of 2001][407]	DHS	Requires cooperation with airport operators and consideration of the use of biometric access control systems for identity verification[408]
Maritime Transportation Security Act of 2002[409]	DHS	Requires biometric credential[410]
Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVRA)[411]	DHS	Border Crossing Card: Section 303(b)(1) requires that "only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers" shall be issued to aliens by October 26, 2004.[412]
Homeland Security Act of 2002 (HSA)[413]	DHS Science and Technology Special Programs Division. The mission of this division is to develop technologies in "Emerging Threats, Risk Sciences, Intelligence, Surveillance, Reconnaissance, and Special Access Programs Control Office."[414]	"In accordance with the Homeland Security Act of 2002, ensuring especially sensitive technologies involving homeland defense are transferred to, or coordinated with, the Under Secretary for S&T [Science & Technology]."[415]

406. *Id.* § 403(c), 115 Stat. at 344 (codified at 8 U.S.C. § 1379 (2006)).

407. Pub. L. No. 107-71, 115 Stat. 597 (2001) (codified at 5 U.S.C. §§ 5313, 8331; 26 U.S.C. § 9502; 31 U.S.C. § 1105; in scattered sections of 49 U.S.C.).

408. *See* Donohue, *supra* note 3, at 438.

409. Pub. L. No. 107-295, 116 Stat. 2064 (2002) (codified at 46 U.S.C. §§ 70101–70117).

410. The TWIC digitalized biometric credential was implemented in 2007 as a result of this Act. *Id.* § 70105, 116 Stat. at 2073.

411. Pub. L. No. 107-173, 116 Stat. 543 (2002) (codified in scattered sections of 8 U.S.C.).

412. *Id.* § 303(b)(1), 116 Stat. at 553 (codified at 8 U.S.C. § 1732 (2006)).

413. Pub. L. No. 107-296, 116 Stat. 2135 (2002) (codified in scattered sections of the

Homeland Security Information Sharing Act (included in Homeland Security Act of 2002)[416]	FBI	Expanded IAFIS to include classified and unclassified information[417]
Help America Vote Act of 2002 (HAVA)[418]	State coordination with SSA.[419]	Section 15483(a) requires each state to implement and maintain an electronic database of all registered voters.[420] HAVA also requires states to verify the identity of the voter registration application through cross-checking the applicant's driver's license or last four digits of the applicant's Social Security Number.[421] If the individual has neither number, the state is required to assign a voter ID number to the applicant.[422]
FAA Reauthorization Bill (Federal Aviation Administration Reauthorization Bill, also known as Vision 100—Century of Aviation Reauthorization Act of 2003)[423]	TSA	CAPPS2 (Computer Assisted Passenger Prescreening System) (now Secure Flight).[424] Relies upon the Passenger Name Record database (PNR). Checks the passenger's data against

U.S.C.).

414. *Science and Technology Special Programs Division*, U.S. DEP'T HOMELAND SEC., http://www.dhs.gov/xabout/structure/gc_1239044157050.shtm.

415. *Id.*

416. 6 U.S.C. § 481 (2006).

417. *See* Donohue, *supra* note 3, at 441.

418. Pub. L. No. 107-252, 116 Stat. 1666, 1666–1730 (2002) (codified as amended at 42 U.S.C. §§ 15301–15545 (2006)).

419. Implementation of HAVA requires state agency tasked with overseeing election rules and procedures for that state to coordinate with SSA in SSN database screening. *See President Signs H.R. 3295, "Help America Vote Act of 2002,"* SOC. SEC. ADMIN. (Nov. 7, 2002), http://www.ssa.gov/legislation/legis_bulletin_110702.html.

420. 42 U.S.C. § 15483(a) (2006).

421. *Id.* § 15483(a)(5)(A)(i).

422. *Id.* § 15483(a)(5)(A)(ii).

423. Pub. L. No. 108-176, 117 Stat. 2490 (2003) (codified as amended in scattered sections of the U.S.C.).

424. *Id.* at §§ 607–608, 117 Stat. at 2568–70 (codified as amended at 49 U.S.C. § 44903 (2006 & Supp. 2010)) (CAPPS2); Secure Flight Program, 73 Fed. Reg. 64,018 (Oct. 28,

		the TSA "No-Fly List," FBI lists, and assigns a terrorist "risk score" through statistical algorithms.[425]
Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)[426]	TSA	Secure Flight[427] passenger prescreening program through PNR database and other databases. Also requires the President to establish an information sharing environment.[428]
Real ID Act of 2005 (REAL ID)[429]	TSA	REAL ID requires technological enhancements and data gathering requirements for driver's licenses. Directs state DMVs to adopt practices that permit centralization of data. Requires production of ID documents to DMV prior to issuance of license. Many states are requiring SAVE immigration-related database screening before issuing driver's licenses.[430]
DNA Fingerprint Act of 2005[431]	FBI	Requires the submission of DNA samples by all citizens and noncitizens in detention as a result of any arrest or apprehension, including misdemeanors,

2008) (to be codified at 49 C.F.R. pts. 1540, 1544, &1560) (Secure Flight).

425. Press Release, U.S. Dep't Homeland Sec., Fact Sheet CAPPS II: Myths and Facts (Feb. 12, 2004), *available at* http://www.techlawjournal.com/agencies/dhs/capps/20040212b.asp.

426. Pub. L. No. 108-458, 118 Stat. 3638 (2004) (codified as amended in scattered sections of the U.S.C.).

427. Secure Flight Program, 73 Fed. Reg. 64,018, 64,019 (Oct. 28, 2008) (to be codified at 49 C.F.R. pts. 1540, 1544, & 1560)

428. *See* Donohue, *supra* note 3, at 456.

429. Pub. L. No. 109-13, 119 Stat. 302 (2005) (codified as amended in scattered sections of 8, 49 U.S.C.).

430. *See id*. at § 202, 119 Stat. at 312 (codified at 49 U.S.C. § 30301 (2006)).

431. Pub. L. No. 109-162, 119 Stat. 3084 (2006) (codified as amended in scattered sections of 42 U.S.C).

		made under federal authority.[432]
Deficit Reduction Act of 2005 (DRA)[433]	Department of Health and Human Services (HHS)[434]	Requires identity verification through presentation of original identity documents (birth certificate) to state officials before the administration of Medicare/Medicaid benefits.[435]
Adam Walsh Child Protection and Safety Act of 2006 (Adam Walsh Act)[436]	FBI[437]	Allows for the tracking of sex offenders with GPS technology.[438] Requires compilation of national database registry that includes the Social Security Number, address, employment information, and license plate number of registered vehicles of sex offenders.[439]
Children's Health Insurance Program Reauthorization Act of 2009 (CHIP)[440]	HHS	Requires verification of identity and citizenship status through database screening prior to issuing benefit.[441]
Patient Protection and Affordable Care Act of 2010 (ACA or Obama Health Care Plan)[442]	HHS	Requires verification of identity and citizenship status through database screening prior to issuing

432. *Id.* § 1004, 119 Stat. at 3085–86 (codified as amended in scattered sections of 42 U.S.C).

433. Pub. L. No. 109-171, 120 Stat. 4 (2006) (codified as amended in scattered sections of U.S.C.).

434. Under implementation of DRA, state benefit granting agencies are charged with distributing Medicare/Medicaid benefits. *Id.*

435. § 6036, 120 Stat. at 80 (codified as amended at 42 U.S.C. § 1396b (2006 & Supp. 2010)).

436. Pub. L. No. 109-248, 120 Stat. 587 (2006) (codified at 42 U.S.C. §§ 16911–16929 (2006 & Supp. 2010)).

437. Under implementation of Adam Walsh Act, state parole boards must monitor release of sex offenders. *Id.* § 112, 120 Stat. at 593.

438. § 621, 120 Stat. at 633–34 (codified at 42 U.S.C. § 16981 (2006 & Supp. 2010)).

439. §§ 114, 119, 120 Stat. at 594, 596 (codified at 42 U.S.C. §§ 16914, 16919 (2006)).

440. Pub. L. No. 111-3, 123 Stat. 8 (2009) (codified in scattered sections of the U.S.C.).

441. *Id.* at § 211, 123 Stat. at 49 (codified at scattered sections of 42 U.S.C.).

		benefit.[443]

Preexisting biometric data collection protocols and the policy drive to expand biometric databases appear to create policy and program synergies between biometric dataveillance programs. It appears that the mandatory expansion of S-COMM, for example, was coordinated with the implementation of the FBI's Next Generation Identification (NGI) program.[444] Under the FBI's NGI project, the government has announced its attempt to institute a comprehensive, centralized, and technologically interoperable biometric database that spans across military and national security agencies, as well as all other state and federal government agencies.[445] Once complete, NGI will strive to centralize whatever biometric data is available on all citizens and noncitizens in the United States and abroad, including information on fingerprints, DNA, iris scans, voice recognition, and facial recognition data captured through digitalized photos, such as U.S. passport photos and REAL ID driver's licenses.[446] The NGI Interstate Photo System, for instance, aims to aggregate digital photos from not only federal, state, and local law enforcement, but also digital photos from private businesses, social networking sites, government agencies, and foreign and international entities, as well as acquaintances, friends, and family members.[447]

Table 17 lists some of the components of the NGI program, demonstrating how the FBI is attempting to implement a national coordinated biometric identification system through the interoperability of multiple digitalized biometric data identifiers. Media reports have identified the FBI's interest in expanding NGI's biometric databases as an underlying motivation for the rapid mandatory expansion of S-COMM through administrative actions by DHS.[448]

Table 17. Examples of Components of FBI's Next Generation Identification (NGI)

NGI Subcomponent	Description
Repository for Individuals of Special Concern (RISC)	Database of records of known or suspected terrorists, wanted persons, registered sex

442. Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified at 42 U.S.C. § 18081 (Supp. 2010)).

443. *Id.* at § 1411, 124 Stat. 224.

444. Tana Ganeva, *5 Things You Should Know About the FBI's Massive New Biometric Database*, ALTERNET (Jan. 18, 2012), http://www.alternet.org/story/153664/5_things_you_should_know_about_the_fbi's_massive_new_biometric_database.

445. *See* Donohue, *supra* note 3, at 443–51.

446. *See id.* For more information about the FBI's Next Generation Identification project, see *Next Generation Identification*, *supra* note 290; *Beyond Fingerprints: Our New Identification System*, FED. BUREAU INVESTIGATION (Jan. 26, 2009), http://www.fbi.gov/news/stories/2009/january/ngi_012609.

447. *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 300. The media stored by the system includes photographs searchable by using facial recognition technology, as well as photographs of scars, distinct marks, and tattoos. *See Next Generation Identification*, *supra* note 290.

448. Wilson, *supra* note 260; *see also* E-mail chain, FOIA document, FBI-SC-1250–53, at 1251–52 (Feb. 2010), *available at* http://uncoverthetruth.org/wp-content/uploads/2011/07/Additional-NGI-Documents.zip.

	offenders, and other persons of "heightened interest."[449]
Enhanced IAFIS Repository (EIR), includes the Rap Back Service	Repository creates compatibility between existing civil and criminal repositories. Employers may enroll in the "Rap Back Service" which allows the FBI to collect employees' biometric data and to notify employers regarding subsequent criminal, and certain civil, activities of employees.[450]
Interstate Photo System (IPS)	Incorporates media not just from law enforcement, but from private businesses, social networking sites, government agencies, and foreign and international entities, as well as individuals like acquaintances, friends, and family members.[451]
Advanced Fingerprint Identification Technology (AFIT)	Increases the processing capacity, storage capacity, and accuracy of IAFIS. Enables the rapid fingerprint search of the RISC.[452]
National Palm Print System (NPPS)	"[C]entralized repository for palm print data that can be accessed nationwide" by local, state, and federal law enforcement and criminal justice agencies.[453] It will "enable users to search latent palmprints obtained from crime scenes against a national repository, enhancing law enforcement's ability to solve crime."[454]
Disposition Reporting Improvements (DRI)	Provides a more complete criminal history repository and more streamlined methods of transmitting disposition data via the

449. *Privacy Impact Assessment: Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Repository for Individuals of Special Concern (RISC)*, FED. BUREAU INVESTIGATION, http://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngi-risc; *see also* Donohue, *supra* note 3, at 444–45.

450. *See Next Generation Identification*, *supra* note 290. According to one scholar, the Rap Back Service "essentially expands the biometric data collected by the FBI and creates a reporting-back mechanism that may take account of everything from attendance at political rallies, to parking violations, to formal charges related to serious crimes." Donohue, *supra* note 3, at 446 (footnote omitted).

451. *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 300. The media stored by the system includes photographs searchable by using facial recognition technology, as well as photographs of scars, distinct marks, and tattoos. *See Next Generation Identification*, *supra* note 290.

452. *See Next Generation Identification*, *supra* note 290.

453. *Id.*

454. FED. BUREAU OF INVESTIGATION, NEXT GENERATION IDENTIFICATION 2 (2009), *available at* http://www.biometriccoe.gov/_doc/FBI_CJIS_0209_NGI_OnePager020409.pdf.

	Interstate Identification Index, the CJIS Wide Area Network, CD-ROM, and potentially through a direct connection to federal courts.[455]
Iris Recognition Program	Provides iris retrieval, search, and maintenance capabilities to identify "persons of interest."[456]

In summary, identity verification programs, such as E-Verify, and identity determination programs, such as S-COMM and NGI, are rapidly proliferating. They can be fairly characterized as components of a "cardless" national ID system in that they are helping to shape the drive for the development of a universal digitalized biometric database to support a biometric national ID system. Eventually, it is possible that such biometric databases will be used for identity inference programs that utilize the tools of big data cybersurveillance and mass dataveillance in attempts to predict crime and prevent terrorism, such as FAST, and to conduct national security risk assessments, such as the "No-Fly List" program.

CONCLUSION

Recent comprehensive immigration reform proposals have called for the enactment of a universal digitalized national ID system to "secure the border." Either a biometric national ID card—e.g., a multimodal biometric Social Security Card, driver's license, and/or passport—or a biometric E-Verify program would likely require a universal biometric database, requiring the collection and permanent or semipermanent electronic storage of, for example, the digital photos, fingerprints, iris scans, and/or DNA samples of those lawfully present in the United States. The constitutional, technological, social, and economic impact of a universal digitalized biometric ID system implemented on a national scale is difficult to overstate. Identity management systems—and the identity verification, identity determination, and identity inference programs that support such systems—have the potential to profoundly impact a wide range of substantive constitutional rights, privacy and civil rights, the constitutional scheme, and normative principles of governance in a democratic society. Yet, the potential constitutional and other consequences of a digitalized biometric national ID or other "cardless" digitalized identity registration system, and their cybersurveillance capacities, have not been fully researched.[457]

---

455. *Id.*

456. Donohue, *supra* note 3, at 447 (explaining that very little information is known about this program, including how the information is maintained and shared, or at what distance the technology can capture an iris scan).

457. For example, Congress has only begun to consider the electronic privacy safeguards necessary for Internet database screening technologies through electronic privacy legislation, which would attempt to protect against discrimination and data misuse that could relate to a digitalized universal biometric database. *See, e.g.*, Ryan Gallagher, *Ancient Electronic Communications Law May Finally Be Updated To Protect Email Privacy*, SLATE (Mar. 19, 2013, 4:08 PM), http://www.slate.com/blogs/future_tense/2013/03/19/patrick_leahy_

At this stage, a biometric national ID and universal biometric ID database system, utilized for widespread identity verification and identity management purposes, is nothing more than a legislative concept. Based on policy precedent involving the proliferation of database screening programs, however, it is unlikely that a biometric national ID would simply take the form of a digitalized Social Security Card that contains a chip with biometric information. A digitalized biometric national ID system would likely facilitate cybersurveillance and dataveillance through cybersurveillance-24/7 body tracking, dataveillance-360° biographical tracking, and restrict physical and logical access.

Cybersurveillance-24/7 Body Tracking. A digitalized biometric national ID could be used to record our movement or create a virtual security checkpoint by recording our whereabouts at the time of the card swipe or smartphone read (e.g., requiring the biometric national ID to be produced at certain points of entry or exit, like the HSPD-12 PIV card). Or if a biometric national ID or ID smartphone is embedded with GPS-RFID tracking technology, such a system could facilitate 24/7 tracking of anyone who possesses and carries such devices.

Dataveillance-360° Biographical Tracking. Information linked to the data captured through the issuance and usage of such a digitalized biometric national ID system could be used to assess characteristics and patterns of those who possess and use such cards, smartphones, or other digitalized IDs. This could be done indiscriminately, such as through the mass cybersurveillance of ordinary citizens. Or this data could be used to target individuals or classifications of individuals—such as targeting groups based on immigration status, national origin, credit history, or zipcode—for additional scrutiny or investigation. The government has implied that it can already engage in biographical data surveillance that is more invasive than the geolocational data surveillance that could be pulled from a GPS tracking device.[458] In other words, sensitive behavioral and biographical data is already at the disposal of the government from credit card receipts, cell phone records, magazine subscriptions, income, zipcode, etc.[459] Currently, interlocking databases can yield personally identifiable information or contextual information on an individual as an employee (e.g., E-Verify), recipient of benefits (e.g., SAVE), international traveler (US-VISIT), and consumer (e.g., ChoicePoint consumer database).[460]

---

introduces_legislation_to_update_ancient_electronic_communications.html; Press Release, Congresswoman Suzan DelBene, DelBene Co-Sponsors Bill with Rep. Lofgren To Reform Electronic Communications Privacy Act (Mar. 6, 2013), *available at* http://delbene.house.gov/press-release/delbene-co-sponsors-bill-rep-lofgren-reform-electronic-communications-privacy-act.

458. Transcript of Oral Argument at 16:9–16, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf (Roberts, C.J.: "Well, you're talking about the difference between seeing a little tile and seeing a mosaic. The one gives you information; the other doesn't." Dreeben, Deputy Solicitor General: "So does a pen register. So does a garbage pull. So does looking at everybody's credit card statement for a month. All of those things this Court has held are not searches.").

459. *See, e.g.*, Cate *supra* note 34, at 440–44, 457–60; Solove *supra* note 34, at 343–45, 357.

460. Through current databases, the government can seek private informational databases, such as ChoicePoint, which collects data on consumer habits, credit reports, etc.

Restricting Physical and Logical Access. Protocols for ID production and inspection are currently implemented to restrict access to certain rights, benefits, and privileges. These identity verification programs are promulgated to satisfy requirements that identity, and citizenship or immigration status, has been established prior to granting the right to work, right to vote, right to access a driver's license, etc. Such a digitalized biometric national ID system would likely be used to determine, for example, whether an individual is an unauthorized immigrant through E-Verify or HAVA, unauthorized for federal benefits through SAVE, and unauthorized for ground or air travel through REAL ID and the "No-Fly List." In addition, like the PIV card issued to federal government employees and federal contractors pursuant to HSPD-12, one day, a digital biometric card could be used to restrict both physical access (e.g., card read to enter buildings and offices) and to restrict logical access (e.g., card read to access computer and Internet).

In other words, a digitalized biometric national ID, including a "cardless" ID system, could facilitate exponentially the convergence of 24/7 cybersurveillance-body tracking and 360° dataveillance-biographical tracking through an automated and coordinated data infrastructure. The potential integration of GPS-RFID tracking into everyday ID documents, and the potential transformation of smartphones into ID devices, forces a consideration of the cybersurveillance and dataveillance implications of these emerging technologies. Those technologies will test the current Fourth Amendment doctrine because they enable the insertion of what is in effect a tracking device into identity cards and phones that citizens will carry voluntarily or by law in their pockets, wallets, and purses. Further, a digitalized ID that is machine readable and that must be produced for identity verification purposes will further dataveillance capacities through compulsory data collection (e.g., centralized, comprehensive biographical database on all citizens and noncitizens) and data accumulation and database aggregation (e.g., each card swipe or each time an ID or smartphone read is recorded digitally, such a read creates both a data record and an opportunity to integrate or aggregate existing data on an individual). The Fourth Amendment doctrine, therefore, must now evolve in the face of modern surveillance technologies and a new dawn of identity management systems and bureaucratized cybersurveillance.

Choicepoint, EPIC, http://epic.org/privacy/choicepoint/. "The Justice Department (DOJ) has signed a $67 million contract with ChoicePoint to provide the FBI, Immigration and Naturalization Service, Border Patrol and other law enforcement agencies with access to ChoicePoint's 13 billion files." *ChoicePoint Sells Personal Data to U.S.*, PEOPLE'S WORLD (May 7, 2003), http://transitional.pww.org/choicepoint-sells-personal-data-to-u-s/.

APPENDIX A: LIST OF TABLES

APPENDIX B: LIST OF ACRONYMS AND KEY TERMS

ABIS *(Automated Biometrics Identification System) (DoD and DoS)*
CBP *(U.S. Customs and Border Protection/DHS)*
CCTV *(Closed Circuit Television Surveillance Video Cameras)*
CODIS *(Combined DNA Index System) (FBI/DOJ)*
DHS *(U.S. Department of Homeland Security)*
Digitalized ID and Digitalized Biometric ID *(Can refer to either ID card or "cardless" identification system)*
DMV *(States' Department [or Division] of Motor Vehicles)*
DOC *(U.S. Department of Commerce)*
DoD *(U.S. Department of Defense)*
DOJ *(U.S. Department of Justice)*
DoS *(U.S. Department of State)*
Drones *(Unmanned Aerial Vehicles)*
E-Verify *(Identity verification through Internet-driven database screening) (DHS and SSA)*
FAST *(Future Attribute Screening Technology) (DHS)*
FBI *(Federal Bureau of Investigation/DOJ)*
GPS *(Global Positioning System)*
HAVA *(Help America Vote Act of 2002, setting forth SSN database screening protocols in an attempt to ensure integrity of voter registration)*
HSPD *(Homeland Security Presidential Directive)*
HSPD-12 *(Policy for a Common Identification Standard for Federal Employees and Contractors)*
ICE *(U.S. Immigration and Customs Enforcement/DHS)*
IDENT *(Automated Biometric Identification System) (DHS)*
IAFIS *(Integrated Automated Fingerprint Identification System) (FBI/DOJ)*
NCIC *(National Crime Information Center) (FBI/DOJ)*
NIST *(National Institute of Standards and Technology/DOC)*
NGI *(Next Generation Identification) (FBI/DOJ)*
NUMIDENT *(Numerical Identification) (SSA's SSN database)*
OPM *(Office of Personnel Management/White House)*
PIV Card *(Personal Identity Verification Card) (Mandated by HSPD-12 for federal employees and federal government contractors)*
RFID *(Radio Frequency Identification)*
SAVE *(Systematic Alien Verification for Entitlements) (USCIS/DHS)*
S-COMM *(Secure Communities) (ICE/DHS)*
SEVIS *(Student and Exchange Visitor Information System) (DHS)*
SSA *(Social Security Administration)*
SSN *(Social Security Number)*
TSA *(Transportation Security Administration/DHS)*
USCIS *(U.S. Citizenship and Immigration Services/DHS)*
US-VISIT *(United States Visitor and Immigrant Status Indicator Technology) (National Protection and Program Directorate/DHS)*