Florida Law Review

Volume 67 | Issue 5 Article 5

March 2016

Big Data Blacklisting

Margaret Hu

BIG DATA BLACKLISTING

*Margaret Hu**

Abstract

"Big data blacklisting" is the process of categorizing individuals as administratively "guilty until proven innocent" by virtue of suspicious digital data and database screening results. Database screening and digital watchlisting systems are increasingly used to determine who can work, vote, fly, etc. In a big data world, through the deployment of these big data tools, both substantive and procedural due process protections may be threatened in new and nearly invisible ways. Substantive due process rights safeguard fundamental liberty interests. Procedural due process rights prevent arbitrary deprivations by the government of constitutionally protected interests. This Article frames the increasing digital mediation of rights and privileges through government-led big data programs as a constitutional harm under substantive due process, and identifies the obstruction of core liberties with big data tools as rapidly evolving and systemic.

---

* Assistant Professor of Law, Washington and Lee University School of Law. I would like to extend my deep gratitude to those who graciously offered comments on this draft, or who offered perspectives and expertise on this research through our thoughtful discussions: John Bagby, Jack Balkin, Kate Bartlett, Lawrence Baxter, Jody Blanke, Joseph Blocher, danah boyd, Franziska Boehm, Rachel Brewster, Sam Buell, Howard Chang, Guy Charles, Andrew Christensen, Danielle Citron, Adam Cox, Jennifer Daskal, Josh Fairfield, Susan Franck, Michael Froomkin, Mark Graber, Jennifer Granick, David Gray, Mark Grunewald, Woody Hartzog, Janine Hiller, Jeff Kahn, Anil Kalhan, Margot Kaminski, Orin Kerr, J.J. Kidder, Anne Klinefelter, Robert Koulish, Corinna Lain, Stephen Lee, Maggie Lemos, Sandy Levinson, Rachel Levinson-Waldman, Jamie Longazel, Erik Luna, Tim MacDonnell, Peter Margulies, Russ Miller, Steve Miskinis, Hiroshi Motomura, Brian Murchison, Mark Noferi, Jeff Powell, Angie Raymond, David Robinson, Mark Rush, Pam Saunders, Mark Seidenfeld, Andrew Selbst, Victoria Shannon, Shirin Sinnar, Ben Spencer, Juliet Stumpf, Dan Tichenor, Steve Vladeck, Russ Weaver, John Weistart, Ben Wittes, Ernie Young, and apologies to those whom I may have inadvertently failed to acknowledge. In addition, this research benefited greatly from the discussions generated from the 2015 *8th Annual Privacy Law Scholars Conference*, co-hosted by Berkeley Center for Law & Technology and George Washington Law; 2015 *Law and Ethics of Big Data* Research Colloquium, hosted by University of Indiana; 2015 *Culp Colloquium*, hosted by the Duke Law Center on Law, Race and Politics; 2015 *Constitutional Law Schmooze on "The Public/Private"*, hosted by Francis King Carey School of Law University of Maryland; 2014 Washington College of Law, American University, Faculty Workshop; 2014–2015 *Emroch Faculty Colloquy Series*, Richmond School of Law; *Transnational Dialogue on Surveillance Methods*, hosted by Max Planck Institute; 2013 Earle Mack School of Law, Drexel University, Faculty Workshop; and the 2013 Duke Law Summer Faculty Workshop. Much gratitude to the *Florida Law Review* for their editorial care, including Trace Jackson, Editor in Chief, and Megan Testerman, Executive Managing Editor. Many thanks to the research assistance of Rossana Baeza, Emily Bao, Lauren Bugg, Russell Caleb Chaplain, Jessica Chi, Cadman Kiker, Kirby Kreider, Oscar Molina, Markus Murden, Kelsey Peregoy, Joe Silver, and Cole Wilson. All errors and omissions are my own.

To illustrate the mass scale and unprecedented nature of the big data blacklisting phenomenon, this Article undertakes a significant descriptive burden to introduce and contextualize big data blacklisting programs. Through this descriptive effort, this Article explores how a commonality of big data harms may be associated with nonclassified big data programs, such as the No Work List and No Vote List—programs that the government uses to establish or deny an individual's eligibility for certain benefits or rights through database screening. The big data blacklisting harms of big data tools to make eligibility decisions are not, of course, limited to nonclassified programs. This Article also suggests how the same consequences may be at play with classified and semi-classified big data programs such as the Terrorist Watchlist and No Fly List. This Article concludes that big data blacklisting harms interfere with and obstruct fundamental liberty interests in a way that now necessitates an evolution of the existing due process jurisprudence.

INTRODUCTION

This Article addresses an emerging constitutional harm in the digital age: the mass "blacklisting"[1] of individuals through the development and adoption of governance tools that rely upon the technologies of big data.[2]

---

1. The term "blacklist" is defined as "a list of persons or organizations under suspicion, or considered untrustworthy, disloyal, etc, [especially] one compiled by a government or an organization." COLLINS ENGLISH DICTIONARY (10th ed. 2012). The concept of "blacklisting" is often associated with 1950s-era McCarthyism. *See, e.g.*, ELLEN SCHRECKER, THE AGE OF MCCARTHYISM: A BRIEF HISTORY WITH DOCUMENTS 92–93 (1994) (explaining that McCarthy-era blacklisting consequences were often economic in nature, leading to unemployment; yet, "[t]he blacklist took a personal toll as well. Broken health and broken marriages, even suicides were not unknown."). Several scholars and experts have analogized the blacklisting practices of the prior historic era with contemporary terrorism prevention practices. *See, e.g.*, JEFFREY KAHN, MRS. SHIPLEY'S GHOST: THE RIGHT TO TRAVEL AND TERRORIST WATCHLISTS 8 (2013) (comparing U.S. passport and travel restrictions during the McCarthy era with the No Fly List restrictions after 9/11, and concluding that "[t]he mistakes of the mid-twentieth century are being remade at the start of the twenty-first century"); David Cole, *The Difference Prevention Makes: Regulating Preventive Justice*, 9 CRIM. LAW & PHIL. 501 (2015) (discussing legal rules that remain in effect that "reflect lessons learned from the McCarthy era, in which thousands of innocent citizens were caught up in the preventive frenzy of anti-communism") (citing Geoffrey Stone, PERILOUS TIMES: FREE SPEECH IN WARTIME: FROM THE SEDITION ACT OF 1798 TO THE WAR ON TERRORISM 311–426 (2004)); Aaron H. Caplan, *Nonattainder as a Liberty Interest*, 2010 WIS. L. REV. 1203, 1205–06 (describing the No Fly List and other government efforts to target suspicious individuals or suspicious behaviors as contemporary "government blacklists" and "blacklisting" programs); Daniel J. Steinbock, *Designating the Dangerous: From Blacklists to Watch Lists*, 30 SEATTLE U. L. REV. 65, 68 (2006) ("It is, therefore, time to ask if something equivalent to the blacklists of fifty years ago is happening again, and, if so, how the twenty-first century use of watch lists [in the post-9/11 counter-terrorism context] might or might not resemble the blacklisting of the McCarthy era.").

2. "Big data" is difficult to define, as it is a newly evolving field and the technologies that it encompasses are evolving rapidly as well. *See generally* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND

Specifically, "big data blacklisting"[3] describes the harm incurred by those categorized by the government as administratively "guilty until proven innocent" by virtue of digitally generated suspicion, such as through government-led big data systems that flag suspicious digital data and database screening results.[4] Those who may be digitally blacklisted include anyone with a digital trail or a presence within a database.

Big data blacklisting harms result from the mediation of and interference with fundamental liberty interests. Additionally, as this Article illustrates, those tracked and isolated for action by government-led big data blacklisting programs often have limited to nonexistent options to remediate or may face consequences without any knowledge of the big data blacklisting program that impacts them.[5] People in this

---

THINK (2013). Thus, some experts have explained that "'Big Data' is a generalized, imprecise term that refers to the use of large data sets in data science and predictive analytics." Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96 (2014). "Technologists often use the technical '3-V' definition of big data as 'high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.'" Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 394 (2014) (quoting *IT Glossary: Big Data*, GARTNER, http://www.gartner.com/it-glossary/big-data/ (last visited Oct. 16, 2015)); *see id*. (citing Doug Laney, *3D Data Management: Controlling Data Volume, Velocity, and Variety*, GARTNER (Feb. 6, 2001), http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf). Multiple authors have addressed the characteristics of "big data" and the challenges posed by big data technologies. *See infra* Part I.A.

3. The use of the term "blacklisting" in the media to describe the consequences of digital watchlisting appears to demonstrate a wider public acknowledgement of and public discourse on the potential consequences of such watchlisting. *See, e.g.*, Meghan Keneally, *Secret Blacklist Stopping Muslim Residents from Becoming Citizen, Lawsuit Claims*, ABC NEWS (Aug. 12, 2014, 6:08 AM), http://abcnews.go.com/US/secret-blacklist-stopping-muslim-residents-citizens-lawsuit-claims/story?id=24910447; Jeremy Scahill & Ryan Devereaux, *Blacklisted: The Secret Government Rulebook for Labeling You a Terrorist*, INTERCEPT (July 23, 2014, 2:45 PM), https://firstlook.org/theintercept/2014/07/23/blacklisted/; Gail Sullivan, *Why the No-Fly List Was Declared Unconstitutional*, WASH. POST (June 25, 2014), http://www.washingtonpost.com/news/morning-mix/wp/2014/06/25/judge-rules-no-fly-list-unconstitutional/ ("Imagine you're in an airport en route to visit family abroad when suddenly you're surrounded. Then you are detained and interrogated. You not only miss your scheduled flight, but can't get on any other flight. . . . And nobody will tell you why. It's as though you've been blacklisted.").

4. *See infra* Part III.C.

5. Various plaintiffs have alleged in litigation that constitutional harms arise from big data watchlisting and dataveillance–cybersurveillance targeting systems, including database screening systems. Afifi v. Lynch, No. 11-0460(BAH), 2015 WL 1941420, at *1–2 (D.D.C. Apr. 30, 2015) (GPS tracking litigation alleging, *inter alia*, a Fourth Amendment violation); Latif v. Holder, 686 F.3d 1122, 1124, 1126 (9th Cir. 2012) (No Fly List litigation by plaintiffs alleging, *inter alia*, due process violations); Complaint at 1–2, Makowski v. Holder, No. 12-cv-05265 (N.D. Ill. July 3, 2012) (Secure Communities (S-COMM) litigation by plaintiff alleging, *inter alia*, a violation of the Privacy Act); Ariz. Contractors Ass'n, Inc. v. Napolitano, 526 F. Supp. 2d 968, 977 (D. Ariz. 2007), *aff'd sub nom.* Chamber of Commerce v. Whiting, 131 S. Ct. 1968 (2011) (E-Verify

category include, most prominently, those who find themselves on a government digital watchlisting program or in a database screening system. These programs rely upon a big data approach to policy making: the incorporation of big data tools into programs that may include mass data collection,[6] data mining,[7] mass digital indexing,[8] database screening protocols,[9] digital watchlisting,[10] big data integration,[11] and predictive analytics.[12]

---

litigation by the U.S. Chamber of Commerce, et al., alleging, *inter alia*, Fourth Amendment violation through search and seizure of data).

6. *See, e.g.*, EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 5 (2014) [hereinafter PODESTA REPORT], *available at* https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf ("[D]ata collection and analysis is being conducted at a velocity that is increasingly approaching real time, which means there is a growing potential for big data analytics to have an immediate effect on a person's surrounding environment or decisions being made about his or her life.").

7. The nature of the impact of government data mining has formed the basis of extensive and important research in recent years. *See, e.g.*, Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 437 (2008); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 321 (2008); Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 343–44 (2008).

8. *See, e.g.*, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1107 (2002) ("[B]y obtaining private sector records, the government can conduct the type of 'fishing expeditions' that the Framers feared.").

9. *See, e.g.*, SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 43–59 (2000) (discussing the history of the use of data markers through computerization that increasingly allows for government identification of one individual against others through database screening of, for example, digitalized fingerprints and DNA); MARTIN KUHN, FEDERAL DATAVEILLANCE: IMPLICATIONS FOR CONSTITUTIONAL PRIVACY PROTECTIONS 2–6 (2007) (examining constitutional implications of "knowledge discovery in databases" (KDD applications) through dataveillance).

10. *See, e.g.*, Sharon Bradford Franklin & Sarah Holcomb, *Watching the Watch Lists: Maintaining Security and Liberty in America*, HUM. RTS., Summer 2007, at 18; KAHN, *supra* note 1; WILLIAM J. KROUSE & BART ELIAS, CONG. RESEARCH SERV., RL33645, TERRORIST WATCHLIST CHECKS AND AIR PASSENGER PRESCREENING (2009); Anya Bernstein, *The Hidden Costs of Terrorist Watch Lists*, 61 BUFF. L. REV. 461, 466 (2013); Peter M. Shane, *The Bureaucratic Due Process of Government Watch Lists*, 75 GEO. WASH. L. REV. 804, 809–10 (2007) ("It ought to be viewed as intolerable in a democratic society for large numbers of innocent citizens to suffer stigmatic government action under a largely secret program, even if such cases can be 'redressed' through individual review."); Steinbock, *supra* note 1, at 78; Susan Stellin, *Who Is Watching the Watch Lists?*, N.Y. TIMES (Nov. 30, 2013), http://www.nytimes.com/2013/12/01/sunday-review/who-is-watching-the-watch-lists.html.

11. Xin Luna Dong & Divesh Srivastava, *Big Data Integration*, 6 PROC. OF VERY LARGE DATA BASES [VLDB] ENDOWMENT 1188, 1189 (describing multiple technologies that assist in big data integration techniques, including schema mapping, record linkage, data fusion, and big data architecture), *available at* http://www.vldb.org/pvldb/vol6/p1188-srivastava.pdf.

12. *See, e.g.*, STEVEN FINLAY, PREDICTIVE ANALYTICS, DATA MINING AND BIG DATA: MYTHS, MISCONCEPTIONS, AND METHODS 3 (2014) (explaining that tools of predictive analytics are not only deployed by the private and commercial sectors, but that "government and other non-profit organizations also have reasons for wanting to know how people are going to behave and

Thus, the interrelationship between various government big data programs, which may on their face appear wholly unrelated, deserves close interrogation. Big data technologies utilized by the government can create a commonality of big data consequences. This Article shows how constitutional harms may attach to this commonality of big data consequences. These big data programs should be viewed collectively and not individually to better understand these consequences. These consequences often afford limited, inadequate, and impractical legal recourse for those impacted by big data-generated inferential guilt or by the type of heightened suspicion that big data technologies can facilitate, as well as for those who find themselves harmed by these digital watchlisting and database screening programs.

It is important to note that big data blacklisting consequences are not limited to programs operating in the public sphere, and remedies may not be restricted to those available in public law.[13] Yet, because this Article focuses on constitutional concerns, it does not attempt to address private big data blacklisting harms. Additionally, while critical of governmental big data cybersurveillance and mass dataveillance systems and methods, this Article is not a blanket rejection of big data tools. Legitimate and valuable uses for big data tools exist in many important contexts.

Introducing the phenomenon of big data blacklisting and its consequences presents other inherent challenges. The phenomenon is new and technologically derived; therefore, it requires a significant descriptive effort to establish the contours of the phenomenon in the first instance. Consequently, this Article includes neither the detail of programmatic description nor the specificity of legal analysis that would be achievable if one chose to critique each program separately. A collective critique of the big data impact of multiple big data blacklisting programs is limited to a discussion as practicable within a single Article.

---

then taking action to change or prevent it"); ERIC SIEGEL, PREDICTIVE ANALYTICS: THE POWER TO PREDICT WHO WILL CLICK, BUY, LIE, OR DIE 59–60 (2013) (discussing predictive policing methods); NATE SILVER, THE SIGNAL AND THE NOISE: WHY SO MANY PREDICTIONS FAIL—BUT SOME DON'T 417–18 (2012) (discussing governmental efforts to isolate relevant signals in correcting the failed attempts to prevent the terrorist attacks of 9/11: "In cases like these, what matters is not our signal *detection* capabilities . . . . We need signal *analysis* capabilities to isolate the pertinent signals from the echo chamber.").

13. *See, e.g.*, FRANK PASQUALE, THE BLACK BOX SOCIETY 101–03 (2015) (describing private credit scoring regimes and computerization of the finance sector); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 3–4 (2014) [hereinafter Citron & Pasquale, *The Scored Society*] (discussing algorithmic and scoring systems implemented by various individuals or companies that use data to make decisions on characterizing a person in numerous aspects of society).

Moreover, analyzing these programs—many of which are classified or semi-classified[14] and may rely upon largely undisclosed policies and big data technologies, such as undisclosed algorithms—entails an unavoidable degree of speculation. But understanding big data blacklisting as a liberty-depriving constitutional harm necessitates a collective critique of multiple programs. As a result, this Article undertakes a significant descriptive burden to provide the necessary backdrop to begin conceptualizing a legal framework capable of remediating big data blacklisting consequences. Within that framework, this Article proposes that a substantive due process analysis is more appropriate than a procedural due process analysis, which may appear to be the most obvious remedial method.

This Article simply poses the question of whether freedom from big data blacklisting harms should be a cognizable fundamental liberty interest. If courts recognized such an interest, then the focus of the constitutional inquiry becomes whether big data blacklisting has occurred. With this as the leading question, the issue of whether big data blacklisting results in a deprivation of an already cognizable fundamental liberty interest would become a secondary concern. This is because any secondary deprivation—such as a restriction on the right to travel—would be ancillary to the primary deprivation. In other words, big data blacklisting would be, in and of itself, the primary deprivation of liberty. Under this theory, courts would construe big data blacklisting harms as an infringement upon a fundamental liberty interest through the obstruction, interference, and technological mediation of freedoms, rights, and privileges generally.[15]

This Article first discusses big data blacklisting as a constitutionally cognizable harm. Part I of this Article explores, in an introductory manner, the appropriateness of both procedural and substantive due process as possible legal frameworks for vindicating big data blacklisting harms. It argues that big data blacklisting systems create an administrative and noncriminal "guilty until proven innocent" concern for the digitally blacklisted. The process of big data blacklisting and the digital suspicion it creates are an infringement upon a fundamental liberty interest.

---

14. For the purposes of this Article, certain programs, such as the Terrorist Watchlist and No Fly List are referred to as classified or semi-classified. While these programs themselves are not technically classified, the government has explained that these programs are informed by classified information. "The term 'classified information' means information which . . . is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution." 18 U.S.C. 798(b) (2012).

15. *See, e.g.*, Caplan, *supra* note 1, at 1209 ("[C]ourts have considered many . . . claims" concerning "the freedom to perform desired actions . . . .").

Additionally, this Article seeks to establish a preliminary factual record of a representative sample of big data blacklisting programs, their functionality, and observed harms and deprivations resulting from their use. Part II provides an overview of the mechanics and structure of nonclassified programs such as the No Work List (i.e., database screening through E-Verify to conduct work eligibility assessments),[16] the No Vote List (i.e., database screening to conduct voter purges from voter registration rolls through Systematic Alien Verification for Entitlements (SAVE),[17] Help America Vote Act (HAVA),[18] etc.), and the No

16. E-Verify is a "pilot" program jointly operated by the U.S. Department of Homeland Security (DHS) and the Social Security Administration (SSA) that enables employers to screen employees' personally identifiable data (e.g., name, birthdate, and Social Security Number) through government databases over the Internet to "verify" the identity and employment eligibility of the employee. U.S. DEP'T OF HOMELAND SEC., U.S. CITIZENSHIP & IMMIGRATION SERVS., E-VERIFY USER MANUAL FOR EMPLOYERS 1 (2014), *available at* http://www.uscis.gov/sites/default/files/files/nativedocuments/E-Verify_Manual.pdf. E-Verify is referred to as the "Basic Pilot Program" in the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA) and in subsequent congressional action extending its funding. *Id.* at 77–78; Basic Pilot Extension Act of 2001, Pub. L. No. 107-128, 115 Stat. 2407, 2407 (2002) (codified at 8 U.S.C. §§ 1101, 1324a (2012)); Basic Pilot Program Extension and Expansion Act of 2003, Pub. L. No. 108-156, 117 Stat. 1944, 1944 (codified at 8 U.S.C. §§ 1101, 1324a (2012)). For a thorough discussion of E-Verify and its legal implications, see Juliet Stumpf, *Getting to Work: Why Nobody Cares About E-Verify (And Why They Should)*, 2 U.C. IRVINE L. REV. 381 (2012). *See also* Margaret Hu, *Reverse-Commandeering*, 46 U.C. DAVIS L. REV. 535, 564 (2012) (discussing the delegation of employment verification and immigration screening to private entities, such as employers) (citing Stephen Lee, *Private Immigration Screening in the Workplace*, 61 STAN L. REV. 1103, 1130 (2009); Huyen Pham, *The Private Enforcement of Immigration Laws*, 96 GEO. L.J. 777, 780–81 (2008)).

17. In recent years, state election officials have used the SAVE database screening protocol to conduct voter purges. *See infra* Subsection II.A.2; *see also* Fatma Marouf, *The Hunt for Noncitizen Voters*, 65 STAN. L. REV. ONLINE 66 (2012). For more information on the SAVE database screening program, see U.S. DEP'T OF HOMELAND SEC., DHS/USCIS/PIA-006, PRIVACY IMPACT ASSESSMENT FOR THE SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS (SAVE) PROGRAM 12 (2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_save.pdf.

18. *See, e.g.*, Help America Vote Act of 2002 (HAVA), Pub. L. No. 107-252, 116 Stat. 1666, 1666–1730 (2002) (codified as amended at 42 U.S.C. §§ 15301–15545 (2012)). HAVA requires each state to implement and maintain an electronic database of all registered voters. 42 U.S.C. § 15483(a). 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. *Id.* § 15483(a)(5)(A)(i). If the individual does not have either number, the state must assign a voter identification number to the applicant. *Id.* § 15483(a)(5)(A)(ii). Each state election office oversees election rules and procedures for that state in the implementation of HAVA. *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 [hereinafter *President Signs HAVA*]. Excellent research has been conducted in recent years on these emerging developments in election law. *See, e.g.*, Rebecca Green, *Rethinking Transparency in U.S. Elections*, 75 OHIO ST. L.J. 779 (2014); Martha Kropf, *North Carolina*

Citizenship List (i.e., database screening to support immigration detention and deportation under the Prioritized Enforcement Program (PEP),[19] the former Secure Communities (S-COMM) program,[20] etc.). The big data blacklisting harms of digital screening tools to make eligibility decisions are not, however, limited to these nonclassified programs. This Article suggests that the same issues may be at play with classified and semi-classified big data programs. Next, this Article addresses such programs, specifically the No Fly List (i.e., database screening through Secure Flight and other databases for digital watchlist

Election Reform Ten Years After the Help America Vote Act, 12 ELECTION L.J. 179 (2013); Daniel P. Tokaji, *HAVA in Court: A Summary and Analysis of Litigation*, 12 ELECTION L.J. 203 (2013); Daniel P. Tokaji & Paul Gronke, *The Party Line: Assessing the Help America Vote Act*, 12 ELECTION L.J. 111 (2013).

19. DHS Secretary Jeh Johnson announced DHS Prioritized Enforcement Program (PEP) on November 20, 2014, to replace the S-COMM program; however, it appears that the database screening protocols of S-COMM will remain intact under PEP. *See* Memorandum from Jeh Charles Johnson, Sec'y, Dep't of Homeland Sec., to Thomas S. Winkowski, Acting Dir., Immigration & Customs Enforcement, 2 (Nov. 20, 2014), *available at* http://www.dhs.gov/sites/default/files/publications/14_1120_memo_secure_communities.pdf.

20. S-COMM, now renamed PEP, *see id.*, is an interoperability program that facilitates data sharing and database screening protocols between the Federal Bureau of Investigation (FBI), DHS, and local law enforcement agencies. *See Secure Communities*, U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, http://www.ice.gov/secure-communities (last visited Oct. 16, 2015). Important scholarship has addressed multiple legal issues relating to S-COMM in recent years. *See, e.g.*, HIROSHI MOTOMURA, IMMIGRATION OUTSIDE THE LAW 79–83 (2014) (discussing the negative consequences of state and local information gathering in the face of S-COMM); Thomas J. Miles & Adam B. Cox, *Does Immigration Enforcement Reduce Crime? Evidence from Secure Communities*, 57 J.L. & ECON. 937 (2014) (arguing that S-COMM had a limited impact on the reduction of crime); Adam B. Cox & Thomas J. Miles, *Policing Immigration*, 80 U. CHI. L. REV. 87, 110–34 (2013) (discussing the impact of S-COMM as including potential interference with local crime control efforts and facilitating a potential "disparate impact" on specific communities); Christopher N. Lasch, *Rendition Resistance*, 92 N.C. L. REV. 149, 209–16 (2013) (describing the effect of S-COMM as "immigration rendition" and calling into question the legality of immigration detainers under S-COMM). DHS explains that S-COMM is justified by a combination of authorities. *See* Memorandum from Riah Ramlogan, Deputy Principal Legal Advisor, to Beth N. Gibson, Assistant Deputy Dir., U.S. Immigration & Customs Enforcement (Oct. 2, 2010), *available at* http://uncoverthetruth.org/wp-content/uploads/2012/01/Mandatory-in-2013-Memo.pdf. DHS relied upon the following: (1) that 28 U.S.C. § 534(a)(1) and 28 U.S.C. § 534(a)(4) together provide the FBI with authority to share fingerprint data with ICE/DHS; (2) that 8 U.S.C. § 1722 mandates the development of a data sharing system that "enable(s) intelligence and law enforcement agencies to determine the inadmissibility or deportability of an [undocumented immigrant]"; and (3) that 42 U.S.C. § 14616 ratifies information or database sharing between federal and state agencies. *Id.* at 4–6.

nomination)[21] and the Terrorist Watchlist (i.e., database screening through the Terrorist Screening Database (TSDB)).[22]

Part III focuses on how each program screens the general public and subpopulations through big data protocols and, in the process, creates its own class of big data blacklisted individuals. Specifically, it explains how, for example, matches and mismatches in big data systems can lead to inferential guilt that can directly or indirectly categorize individuals as administratively "guilty until proven innocent" by virtue of digitally generated suspicion. The risk of mass, erroneously heightened suspicion that is now facilitated by big data tools places fundamental liberty interests at risk as well.

Part IV contends that substantive due process rights were forged in a small data world.[23] It is now necessary, therefore, to revise the substantive due process inquiry in light of big data challenges and constitutional threats. This Article concludes that the lack of procedural and substantive due process protections in place to safeguard those wrongly facing digital blacklisting and the mass scale of the problem will likely place unprecedented pressure on core constitutional rights.

---

21. For an excellent discussion on the No Fly List, including a careful examination of both the constitutional and human impact, see KAHN, *supra* note 1. Jeffrey Kahn carefully lays out the history and programmatic structure of the No Fly List. *Id.* at 137–53; *see also* Vision 100—Century of Aviation Reauthorization Act, Pub. L. No. 108-176, 117 Stat. 2490, 2568 (2003) (codified as amended at 49 U.S.C. § 44903 (2012)); Secure Flight Program, 73 Fed. Reg. 64,018, 64,019 (Oct. 28, 2008) (codified at 49 C.F.R. §§ 1540, 1544, 1560); Press Release, Transp. & Sec. Admin., TSA to Test New Passenger Pre-Screening System (Aug. 26, 2004), *available at* http://www.tsa.gov/press/releases/2004/08/26/tsa-test-new-passenger-pre-screening-system (describing the implementation of a post-9/11 passenger prescreening program that checks passengers' names against terrorist watchlists to improve the use of "no fly" lists). The Computer Assisted Passenger Prescreening System (CAPPS II) relies upon the Passenger Name Record database (PNR), checks the passenger's data against the Transportation Security Administration's (TSA) "No-Fly" list and the FBI's lists, and assigns a terrorist "risk score" through statistical algorithms. *See* Press Release, U.S. Dep't of Homeland Sec., CAPPS II: Myths and Facts (Feb. 13, 2004), *available at* http://www.hsdl.org/?view&did=478534.

22. The Terrorist Screening Database (TSDB) is "often referred to as the 'Terrorist Watchlist.'" *About the Terrorist Screening Center*, FED. BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, *available at* https://www.fbi.gov/about-us/nsb/tsc/about-the-terrorist-screening-center.

23. "'Small data,' like 'big data,' has no set definition." Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 329 n.6 (2015). Generally, small data can be described as "solving discrete questions with limited and structured data, and the data are generally controlled by one institution." *Id.* (citing JULES J. BERMAN, PRINCIPLES OF BIG DATA: PREPARING, SHARING, AND ANALYZING COMPLEX INFORMATION 1–2 (2013)).

I. OVERVIEW OF THE BIG DATA BLACKLISTING INQUIRY

Before individuals are allowed to fly,[24] work,[25] drive,[26] or vote,[27] citizens and noncitizens alike may now be subjected to mass data collection and automated or semi-automated database screening protocols.[28] Increasingly, in the name of national security and homeland security, post-9/11 big data programs implemented by the government partially obstruct core rights and freedoms in some instances and altogether block them in others.[29] Moreover, because of the virtual nature of mass data collection and database screening, and the classified or semi-

24. *See infra* Subsections II.B.2 and III.B.2.

25. *See infra* Subsections II.A.1 and III.A.1.

26. Prior to issuing driver's licenses, many states now screen individuals through SAVE, a database screening program operated by DHS. *See*, *e.g.*, *Applying for a Driver's License or State Identification Card*, U.S. DEP'T OF HOMELAND SEC. 2, *available at* http://www.ice.gov/doclib/sevis/pdf/dmv_factsheet.pdf (last updated Sept. 5, 2012) ("Most states and territories use the Systematic Alien Verification for Entitlements (SAVE) Program to determine a non-citizen's eligibility for many public benefits, including the issuance of a driver's license.").

27. *See infra* Subsections II.A.2 and III.A.2

28. *See, e.g.*, Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1260 (2007) ("Automated decision systems have been characterized as rules-based programs, data-matching programs, or data-mining programs. . . . [For example,] data-matching systems compare two or more databases with an algorithmic set of rules that determine the likelihood that two sets of personal identifying information represent the same individual." (citing Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 3 (2005)); Citron & Pasquale, *The Scored Society*, *supra* note 13, at 4 ("Automated systems are claimed to rate all individuals in the same way . . . . [However, b]ecause human beings program predictive algorithms, their biases and values are embedded into the software's instructions, known as the source code and predictive algorithms. Scoring systems mine datasets containing inaccurate and biased information provided by people.") (footnote omitted); Michael Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, U. PA. L. REV. (forthcoming) (describing "Automated Suspicion Algorithms" as "machine learning processes [that] seek to predict individual criminality"), *available at* http://ssrn.com/abstract=2593795.

29. Journalist and attorney Glenn Greenwald, and journalist and documentary filmmaker Laura Poitras—who reportedly exercise sole possession over the full Snowden files—and other surveillance experts have shared the view that the Snowden disclosures profoundly implicate questions of democratic governance. GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 6 (2014) ("Will the digital age . . . bring about a system of omnipresent monitoring and control [?]"); Peter Maass, *The Intercept's Laura Poitras Wins Academy Award for 'Citizenfour'*, INTERCEPT (Feb. 22, 2014), *available at* https://firstlook.org/theintercept/2015/02/22/poitras-wins-oscar-for-citizenfour/ ("'The disclosures that Edward Snowden revealed don't only expose a threat to our privacy but to our democracy itself,' Poitras said in her acceptance speech [at the 87th Academy Awards, immediately after Poitras received the Oscar for Best Documentary Feature for directing *Citizenfour*]."); RACHEL LEVINSON-WALDMAN, BRENNAN CTR. FOR JUSTICE, WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA 9 (2013) ("The collection and retention of non-criminal information about Americans for law enforcement and national security purposes poses profound challenges to our democracy and our liberties.").

classified nature of certain programs, the digital mediation of and potential interference with liberty interests can occur without the individual's knowledge or consent.[30]

Many emerging big data cybersurveillance[31] and dataveillance[32] systems have not been fully interrogated. Yet, these big data systems are rapidly proliferating as a post-9/11 policy prescription to assess and prevent potential criminal and terroristic threats.[33] The implications of government-led big data screening programs are especially critical in how they impact those subjected to specific administrative and investigatory actions as a result of the digital screening protocol and data analysis. But these implications are not meaningful in the abstract. To demonstrate this phenomenon and the associated harms, this Article describes the mechanics and consequences of multiple big data cybersurveillance and mass dataveillance programs that purportedly serve homeland security and national security objectives. First, however,

30. *See, e.g.*, PRIVACY AND POWER: A TRANSATLANTIC DIALOGUE IN THE SHADOW OF THE NSA-AFFAIR (Russell A. Miller ed., forthcoming); Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773 (2015); Anjali S. Dalal, *Shadow Administrative Constitutionalism and the Creation of Surveillance Culture*, 2014 MICH. ST. L. REV. 61 (2014); Anil Kalhan, *Immigration Surveillance*, 74 MD. L. REV. 1 (2014); Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843 (2014); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269 (2012); Chris Jay Hoofnagle, *Big Brother's Little Helpers: How Choice Point and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COMM. REG. 595 (2004).

31. *See, e.g.*, LAWRENCE LESSIG, CODE VERSION 2.0, at 209 (2006) (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"). Critically important works published in recent years have helped to illuminate the modern surveillance architecture. *See, e.g.*, JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 17–18 (2014); SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX (2014); DANA PRIEST & WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE (2011); SHANE HARRIS, THE WATCHERS (2010); ROBERT O'HARROW, JR., NO PLACE TO HIDE (2006); JENNIFER STISA GRANICK, BYE, BYE, AMERICAN SPIES: WHAT MODERN SURVEILLANCE IS, WHY YOU SHOULD CARE, AND WHAT TO DO ABOUT IT (forthcoming).

32. *See, e.g.*, Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. ASS'N FOR COMPUTING MACHINERY 498 (1988). Roger Clarke describes dataveillance as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons." *Id.* at 499. *See also* DAVID LYON, SURVEILLANCE STUDIES 16 (2007) ("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 . . . .").

33. *See, e.g.*, Jennifer C. Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327, 328–30 (2014).

Part I attempts to provide background information to help contextualize the big data blacklisting phenomenon.

A. *What Is Big Data Blacklisting?*

Big data blacklisting is the process of categorizing individuals as administratively "guilty until proven innocent" by virtue of suspicious digital data and database screening results.[34] Constitutional liberty interests assumed in a small data world are now threatened in ways that are difficult to grasp. In a small data world, governmental entities were often prevented from digitally mediating rights and liberties due to technological and resource limitations.[35] Thus, freedoms generally could be obstructed only individually or in groups. If they were obstructed en mass, freedoms were often obstructed directly and physically (e.g., mass incarceration and mass internment). In other words, inherent governance and technological limitations generally rendered impracticable mass deprivations, including erroneous mass deprivations, on a scale of millions of individuals based upon digitally generated suspicion or heightened suspicion facilitated by big data tools. This was particularly so within a democratic system designed to enforce strong procedural protections in criminal justice matters.[36]

---

34. It is important to recognize that legal scholars have used the term "blacklist" in a variety of academic contexts. *See, e.g.*, Dawn C. Nunziato, *The Beginning of the End of Internet Freedom,* 45 GEO. J. INT'L L. 383 (2014) (describing the practice of "blacklisting" websites and filtering internet content by governments in the international community and in the United States, and the threat to free speech protections this poses); Katharine A. Van Tassel, *Blacklisted: The Constitutionality of the Federal System for Publishing Reports of "Bad" Doctors in the National Practitioner Data Bank*, 33 CARDOZO L. REV. 2031 (2012) (discussing the risks of infringement of rights of doctors through the use of the National Practitioner Data Bank, a "blacklisting" database for medical professionals); Catherine L. Fisk, *The Role of Private Intellectual Property Rights in Markets for Labor and Ideas: Screen Credit and the Writers Guild of America, 1938-2000*, 32 BERKELEY J. EMP. & LAB. L. 215 (2011) (describing the use of "blacklists" in the industry to distance itself from screenwriters with questionable political views).

35. *See, e.g.*, Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. ONLINE 335 (2014).

36. Cole, *supra* note 1, at 506 ("In theory, the paradigm of prevention is constrained by a number of constitutional principles under U.S. law, including substantive and procedural due process, freedoms of speech and association, equal protection, and the civil-criminal divide. In practice, however, formal constitutional constraints have played a relatively modest role in restricting preventive measures."); Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 1009 (2014) ("Given that Big Data is the aggregation of data about data, and that all data online is handed off to ISPs in some form or another, the foregoing principles have been (over) extended to place the entire Internet outside of meaningful constitutional protections, thereby allowing massive, suspicionless, and even prospective data gathering by government.").

Yet, in what Jack Balkin and Sanford Levinson have termed the "National Surveillance State,"[37] the procedural protections that once operated in traditional administrative and criminal justice matters are at risk.[38] In the National Surveillance State that is rapidly unfolding within the Information Age, it is not so much physical personhood that big data programs threaten but, as Daniel Solove asserts, it is digital personhood and the "digital person" that are at risk.[39] The research of big data scholars[40] and others illuminates the disruptive and transformative nature of big data.

For example, several scholars assert that big data-driven policing methods that are predictive in nature make irrelevant in practice the legal

---

37. *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 12 (2008); Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489, 520–21 (2006) (defining the "National Surveillance State" as being "characterized by a significant increase in government investments in technology and government bureaucracies devoted to promoting domestic security and (as its name implies) gathering intelligence and surveillance using all of the devices that the digital revolution allows").

38. Balkin & Levinson, *supra* note 37, at 523. Jack Balkin and Sanford Levinson explain that, in the National Surveillance State,

> [T]he government can create a parallel law enforcement structure that routes around the traditional criminal justice system with its own rules for surveillance, apprehension, interrogation, detention, and punishment. Because it is not subject to the oversight and restrictions of the criminal justice system, the government may be increasingly tempted to use this parallel system for more and more things. It [the government] may argue that the criminal justice system is outmoded and insufficiently flexible to deal with the types of security problems it now faces. However, the more that the government routes around the criminal justice system, the more it institutionalizes the parallel system as the method of choice.

Id.

39. *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1 (2004) ("It is ever more possible to create an electronic collage that covers much of a person's life—a life captured in records, a digital person composed in the collective computer networks of the world."); *see also id.* at 161 ("Privacy is about degrees of accessibility. The threat to privacy is not in isolated pieces of information, but in increased access and aggregation, the construction of digital dossiers and the uses to which they are put.").

40. *See, e.g.*, danah boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15 INFO. COMM. & SOC'Y 662, 662–79 (2012); ROB KITCHIN, THE DATA REVOLUTION: BIG DATA, OPEN DATA, DATA INFRASTRUCTURES & THEIR CONSEQUENCES xv–xvii (2014); EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM ix–xv (2013); MAYER-SCHÖNBERGER & CUKIER, *supra* note 2; Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 63–64 (2012); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. (forthcoming 2016) (manuscript at 3–6), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899; Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, *supra* note 30, at 775–91.

requirement of reasonable suspicion.[41] Similarly, scholars such as Joshua Fairfield and Erik Luna ask whether the small data "innocence" of criminal defendants now must be recast as big data "digital innocence."[42] Jack Balkin[43] and other experts contend that big data and technologies of surveillance made possible by the Information Society have changed the landscape of governance tools.[44] To assist in grappling with this sea change, Erin Murphy explains that modern technological advances have introduced new governmental "paradigms of restraint"—techniques of punishment and restraint that focus on governance through emerging surveillance developments that do not depend upon physical restraint and

41. *See, e.g.*, Ferguson, *supra* note 23, at 331–32 ("[R]easonable suspicion—as a small data doctrine—may become practically irrelevant in an era of big data policing . . . . [because it] becomes significantly distorted when officers have access to more individualized or predictive information about a suspect."); Elizabeth E. Joh, *Policing by the Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 56 (2014) (questioning, for example, "whether predictive software based on historical crime data is similar to other uses of third party information that have already been held to support a reasonable suspicion determination"); Rich, *supra* note 28, at 5 (explaining that, until the introduction of machine learning technologies, "determining the existence of individualized suspicion—determining whether the historical facts give rise to probable cause or reasonable suspicion—has remained the sole province of human actors") (footnote omitted).

42. Fairfield & Luna, *supra* note 36, at 988–91 (2014) ("The growth of data collection, connection, and parsing capabilities could transform Big Data technologies into an important tool for establishing innocence . . . . [However,] data science and Big Data technologies have been overwhelmingly used to convict.") (citing NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD, 179–80 (2009)). Brandon Garrett argues that, in the criminal procedure context, "[a]s big data "becomes increasingly relevant to criminal cases . . . rules capable of handling complex and Big Data discovery should be developed." Brandon L. Garrett, *Big Data and Due Process*, 99 CORNELL L. REV. ONLINE 207, 208 (2014).

43. *See, e.g.*, Balkin, *supra* note 37, at 12; Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2297 (2014) ("The digital era is different. Governments can target for control or surveillance many different aspects of the digital infrastructure that people use to communicate: telecommunications and broadband companies, web hosting services, domain name registrars, search engines, social media platforms, payment systems, and advertisers.").

44. *See, e.g.*, LYON, *supra* note 32, at 16; David Lyon, *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*, BIG DATA & SOC. 2 (2014) ("[A]s political-economic and socio-technological circumstances change, so surveillance also undergoes alteration, sometimes transformation."); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1949 (2013) (discussing "the risks surveillance poses to democratic self-governance . . . [including] self-censorship, in terms of speech, action, or even belief") (internal citation omitted); JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 175–84 (2005); Jeffrey Rosen, *The Deciders: Facebook, Google, and the Future of Privacy and Free Speech*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 69–82 (Jeffrey Rosen & Benjamin Wittes eds., 2011).

fall outside of the criminal law context.[45] David Cole,[46] Jennifer Daskal,[47] Ian Kerr,[48] and other scholars assert that these new developments in governance methods are preventative and ex ante in nature, and precrime-focused.[49] Cole contends that surveillance is but one tool among many governance tools that now comprises a new "paradigm of prevention" that has been embraced in the aftermath of the terrorist attacks of 9/11.[50] Gabriella Blum and Ben Wittes,[51] and others have described the manner in which technological developments, including surveillance technologies, are now deployed in a way that forces a reconceptualization of the "social contract."[52]

---

45. Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321, 1329 (2008) ("A range of new technologies has greatly enhanced the state's ability to monitor large numbers of individuals. With the advent of surveillance methods less costly than physical restraint, the standard binary of incarceration and liberty has unfurled into a broad continuum on which those two choices mark only the extremes.").

46. Cole, *supra* note 1, at 503 (characterizing "the post-9/11 full-scale adoption of a paradigm of prevention" as "a sea change").

47. Daskal, *supra* note 33, at 331 (explaining that precrime "restrictions share common features: they are targeted at particular individuals, entities, or categories of individuals; they impose noncustodial restrictions; and they are preventive in both purpose and effect").

48. Ian Kerr, *Prediction, Pre-emption, Presumption: The Path of Law After the Computational Turn*, *in* PRIVACY, DUE PROCESS AND THE COMPUTATIONAL TURN: THE PHILOSOPHY OF LAW MEETS THE PHILOSOPHY OF TECHNOLOGY 91–120 (Mireille Hildebrandt & Katja de Vries eds., 2013) (contending that predictive technologies facilitate a philosophy of pre-emption that shifts ex post facto systems of punishment to *ex ante* systems of prevention in a way that threatens due process); s*ee also* Ian Kerr & Jessica Earle, *Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy*, 66 STAN. L. REV. ONLINE 65, 66 (2013).

49. *See, e.g.*, Ferguson, *supra* note 23, at 351; Joh, *supra* note 41, at 56; s*ee also* Mark L. Noferi & Robert Koulish, *The Immigration Detention Risk Assessment*, 29 GEO. IMMIGRATION L. J. 45 (2015) (discussing the "deployment nationwide [of] a new automated risk assessment tool to help determine whether to detain or release noncitizens pending their deportation proceedings").

50. Cole, *supra* note 1, at 501 (explaining that the "paradigm of prevention" includes many tools, including "the use of pretextual charges for preventive detention, the expansion of criminal liability to prohibit conduct that precedes terrorism, and expansion of surveillance at home and abroad").

51. BENJAMIN WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE: ROBOTS AND GERMS, HACKERS AND DRONES—CONFRONTING A NEW AGE OF THREAT 13–14 (2015).

52. *Id.* at 13 (discussing the "conceptual challenges that this new security environment poses—how it disrupts the traditional social contract described by the Enlightenment political theorists, how it forces us to rethink notions of privacy and the relationship between liberty and security within the liberal state, and how it defies the traditional allocation of powers among states over their territories and citizens"); SIMON CHESTERMAN, ONE NATION UNDER SURVEILLANCE: A NEW SOCIAL CONTRACT TO DEFEND FREEDOM WITHOUT SACRIFICING LIBERTY 251–52 (2011) (explaining that surveillance technologies are forcing an evolution of the social contract that "differs from the traditional social contract[,]" and observing that "[p]rivacy theorists and lawyers

Those concerned with surveillance and privacy in the digital age often rely upon the protective potential of the Fourth Amendment of the Constitution. Scholars such as Danielle Citron and David Gray,[53] Laura Donohue,[54] Orin Kerr,[55] Christopher Slobogin,[56] and others[57] have explored the capacity of the Fourth Amendment to address challenges of modern surveillance. Yet, the Fourth Amendment does not generally cover big data systems designed to execute day-to-day bureaucratized surveillance. In light of this, Danielle Citron explains that emerging technologies require an evolution of procedural due process.[58] This evolution must include, for example, greater transparency in describing the underlying algorithms or automated systems that may impact rights and privileges.[59] Kate Crawford and Jason Schultz explain that the predictive harms of big data systems in the private sector require a conceptualization of Citron's technological due process rights when such harms occur.[60]

---

have struggled to respond to these moves, in part because of the diminishing sphere of truly private activity and the growing coercive powers of the state").

53. *See, e.g.*, David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 63–64 (2013); David C. Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 390 (2013).

54. *See, e.g.*, Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 202–19 (2015); Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 863–64 (2014); Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 514–29 (2012).

55. *See, e.g.*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 802–08 (2004).

56. *See, e.g.*, Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1733–42 (2014); Christopher Slobogin, *Making the Most* of United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y. 1, 3–4 (2012).

57. *See, e.g.*, Benjamin Wittes, *Databuse: Digital Privacy and the Mosaic*, BROOKINGS INST. (Apr. 1, 2011), http://www.brookings.edu/research/papers/2011/04/01-databuse-wittes.

58. Citron, *Technological Due Process*, *supra* note 28, at 1281 (2007) (noting that with the advent of automated decisionmaking technologies and "in the automated administrative state, neither due process nor policymaking procedures adequately protect individuals").

59. *See id.* at 1284 ("Access to an automated program's source code—the programmer's instructions to the computer—might provide a meaningful way for individuals to challenge an agency's claims and dispel the influence of automation bias.") (citing Christopher W. Clifton, Deirdre K. Mulligan & Raghu Ramakrishnan, *Data Mining and Privacy: An Overview*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 191, 203 (Katherine Strandburg & Daniela Stan Raicu eds., 2006)).

60. *See, e.g.*, Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 122 (2014) ("Citron's

B. *Big Data Blacklisting and Due Process Liberty Interests*

This Article attempts to extend the discussion on the intersection of due process and big data further by proposing another framework: the remediation of governmental big data blacklisting harms through a substantive due process approach. Big data blacklisting does not yet appear to be a constitutionally cognizable claim or harm under the existing jurisprudence. Yet, big data blacklisting itself is the harm that may be considered unconstitutional when grounded in due process through a conceptualization of what substantive due process rights can and should encompass, in an age when daily existence and governing methods both have been utterly transformed by big data technologies.

It is arguable, in fact, that the United States is on the verge recognizing of such a right. In support of this argument, it is significant to note that several litigants[61] and scholars have recently attempted to define and vindicate this right: to be free of the offense of inclusion on a digital watchlist and to be free of an obstruction of liberty interests that may occur through database screening and other dataveillance or cybersurveillance.[62]

[technological due process] approach could be expanded to address the predictive privacy harms of Big Data.").

61. In multiple recent cases filed in federal court, plaintiffs have alleged constitutionally protected rights are potentially infringed upon by digital watchlisting and, therefore, seek recourse through the removal of their names and records from watchlists and databases. *See, e.g.*, Plaintiff's Petition for Judicial Review at 3, Naim v. Dep't of Homeland Sec., 1:15-cv-00842 (N.D. Ill. Jan. 28, 2015) ("Petitioner respectfully requests confirmation that his name is removed and/or cleared from any of the federal 'watchlists' that may operate to prejudice and/or impede his constitutionally protected liberty interests and his constitutional right to travel."); Plaintiff's Complaint at 2, Abdelfattah v. Dep't of Homeland Sec., 1:07-cv-01842-RCL, ¶ 6 (D.D.C. Oct. 11, 2007) ("This suit seeks an order from this [honorable] court, to order the US government and its defendants [sic] agencies (ICE, CBP, CIS, FBI) to Expunge Plaintiff TECS/IBIS record located in the Treasury Enforcement Communication System know [sic] as (TECS II).").

62. Aaron Caplan, Jennifer Daskal, Jeffrey Kahn, Peter Margulies, Peter Shane, Daniel Steinbock, Juliet Stumpf, Daniel Solove, and others, have proposed more robust constitutional protections and other legal remedies are needed in light of emerging policies and technological developments. Although these scholars do not frame the potential constitutional harms and privacy harms as big data blacklisting harms, they are also concerned with the liberty infringements and restrictions on freedom that are associated with digital watchlisting, database screening, and other bureaucratized surveillance programs. *See, e.g.*, Caplan, *supra* note 1, at 1203–05 (proposing that "the constitutional immunity from bills of attainder[–]that is, the rule against singling out persons for punishment without trial[–]should be recognized as a due process liberty interest," and specifically discussing "government blacklists" like the "No Fly List"); Daskal, *supra* note 33, at 362 (describing the impact of the No Fly List as having "a significant and underappreciated impact on substantive liberty interests"); Jeffrey Kahn, *International Travel and the Constitution*, 56 UCLA L. REV. 271, 276 (2008) (arguing that a fundamental liberty interest in the right for U.S. citizens to travel internationally should be recognized); Shane, *supra* note 10, at 810 (arguing for a "tailoring [of] the formality of post inclusion adjudication (1) to the

The Due Process Clause of the Fifth Amendment states that no person shall "be deprived of life, liberty, or property, without due process of law."[63] The Due Process Clause of the Fourteenth Amendment further states that no state shall "deprive any person of life, liberty, or property, without due process of law."[64] The Due Process Clauses of the Fifth and Fourteenth Amendments encompass both a procedural and a substantive component. Erwin Chemerinsky explains the distinction between procedural and substantive due process in the following way:

> [S]trangely enough, if you look through Supreme Court opinions you will never find a definition [of substantive due process]. Substantive due process asks the question of whether the government's deprivation of a person's life, liberty or property is justified by a sufficient purpose. Procedural due process, by contrast, asks whether the government has followed the proper procedures when it takes away life, liberty or property. Substantive due process looks to whether there is a sufficient substantive justification, a good enough reason for such a deprivation.[65]

Procedural due process is the concept that when the government deprives a citizen of an interest in life, liberty, or property, it must give

---

nature of the different claims that may arise and (2) to the level of care exercised to protect the rights of individuals during determinations to list particular individuals at the "front end" of the process"); Steinbock, *supra* note 1, at 68–69 (arguing that potential reforms of the practice of watchlisting could include "narrowing the substantive standard for selection; adding procedural protection, particularly some form of adversarial process; and restricting the uses of watch list results"); Stumpf, *Getting to Work*, *supra* note 16, at 406–07 (arguing for consideration of a potential constitutional liberty interest in preventing obstruction of employment opportunities that may occur through E-Verify database screening, elaborating that: "[T]he liberty interest here is the right not to be deprived of employment through arbitrary government action. Another way of articulating this is to say that deprivation of the freedom to engage in the lawful behavior of working requires due process of law if it is to avoid arbitrariness"); Peter Margulies, *Rage Against the Machine?: Automated Surveillance and Human Rights* 33 (forthcoming 2016) (arguing that "compliance with safeguards would permit tailored reconnaissance and surveillance, while protecting rights") (citation omitted), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2657619; Irina D. Manta & Cassandra Burke Robertson, *Secret Jurisdiction*, EMORY L. J. (forthcoming 2016) *available at* http://http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2647779; *see also* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 98 (2008) ("By understanding privacy as shaped by the norms of society, we can better see why privacy should not be understood solely as an individual right. . . . [P]rivacy protects the individual because of the benefits it confers on society."); SOLOVE, DIGITAL PERSON, *supra* note 39, at 160–61 ("Public records are increasingly posing a serious threat to privacy in the Information Age. . . . The threat to privacy is not in isolated pieces of information, but in increased access and aggregation, the construction of digital dossiers and the uses to which they are put.").

63. U.S. CONST. amend. V.

64. U.S. CONST. amend. XIV, § 1.

65. Erwin Chemerinsky, *Substantive Due Process*, 15 TOURO L. REV. 1501, 1501 (1999).

the citizen notice and an opportunity to be heard.[66] Substantive due process, on the other hand, is not as simple. One expert explains that "Supreme Court decisions often give the impression that substantive due process jurisprudence fits into a simple two-tiered framework. Within this model, government intrusions on so-called 'fundamental' rights are subject to 'strict' or exacting scrutiny, a test sometimes formulated as inquiring whether a burden is necessary to promote a 'compelling state interest.'"[67] Substantive due process rights often appear as a protection of rights that are "deeply rooted in this Nation's history and tradition."[68] Rights that are not "fundamental" or "deeply rooted" are subject to lesser scrutiny. "All other liberty interests may be abridged or abrogated pursuant to a validly enacted state law if that law is rationally related to a legitimate state interest."[69]

The fundamental liberty interests of the preexisting substantive due process doctrine often turn on autonomy, dignity, self-determination, and individual identity.[70] This substantive due process jurisprudence, therefore, is consistent with predominant themes in the contemporary privacy discourse. Increasingly, scholars are examining the concept of the "proliferation of networked identities and selves," which concerns the preservation of the autonomous self within the infrastructure of the Information Society.[71] In addition, scholars such as Anita Allen,[72] Ryan

66. *See* Mathews v. Eldridge, 424 U.S. 319, 332–35 (1976).

67. Richard H. Fallon, Jr., *Some Confusions About Due Process, Judicial Review, and Constitutional Remedies*, 93 COLUM. L. REV. 309, 314 (1993) (footnotes omitted).

68. Washington v. Glucksberg, 521 U.S. 702, 721 (1997).

69. Lawrence v. Texas, 539 U.S. 558, 593 (2003).

70. *See, e.g.*, Obergefell v. Hodges, 135 S. Ct. 2584, 2597–98 (2015) ("In addition these liberties extend to certain personal choices central to individual dignity and autonomy, including intimate choices that define personal identity and beliefs.") (citing Eisenstadt v. Baird, 405 U.S. 438, 453 (1972); Griswold v. Connecticut, 381 U.S. 479, 484–86 (1965); *see also Lawrence*, 539 U.S. at 574 (2003); *Glucksberg*, 521 U.S. at 726 (1997); Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 851 (1992) ("These matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment.").

71. Frank Pasquale & Danielle Keats Citron, *Promoting Innovation While Preventing Discrimination: Policy Goals for the Scored Society*, 89 WASH. L. REV. 1413, 1413–14 (2014) (referring to the work of Professor Tal Z. Zarsky); *see, e.g.*, JULIE COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 20 (2012); Tal Z. Zarsky, *Understanding Discrimination in the Scored Society*, 89 WASH. L. REV. 1375, 1380–81 (2014); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1913 (2013); Tal Z. Zarsky, *Mining the Networked Self*, 6 JERUSALEM REV. LEGAL STUD. 120, 120–21 (2012).

72. *See, e.g.*, Anita L. Allen, *Dredging Up the Past: Lifelogging, Memory, and Surveillance*, 75 U. CHI. L. REV. 47, 66 (2008).

Calo,[73] Danielle Citron and Frank Pasquale,[74] Julie Cohen,[75] Michael Froomkin,[76] Jon Mills,[77] Helen Nissenbaum,[78] Neil Richards,[79] Paul Schwartz,[80] Daniel Solove,[81] and others[82] have examined the intersection of privacy rights with personal and social autonomy rights. The topics of privacy, surveillance, and an evolving due process jurisprudence are each extraordinarily complex. An exhaustive, careful treatment of each goes beyond the scope of this Article. Nonetheless, in support of a substantive due process approach to big data blacklisting harms, it is worth quickly noting that the apparent aims of the modern substantive due process doctrine, and contemporary privacy and surveillance scholarship, may in many ways each complement the other.[83] Scholars such as Mireille

73. *See, e.g.*, M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012); M. Ryan Calo, Essay, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133–35 (2011); M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN ST. L. REV. 809, 811–16 (2010).

74. *See, e.g.*, PASQUALE, *supra* note 13, at 16; Citron & Pasquale, *The Scored Society*, *supra* note 13, at 1419.

75. COHEN, *supra* note 71, at 20; Cohen, *supra* note 71, at 1920–21 (2013).

76. *See, e.g.*, A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1465 (2000).

77. *See, e.g.*, JON L. MILLS, PRIVACY: THE LOST RIGHT 15 (2008) ("We give up the right to make many decisions as part of the social contract. Being a citizen grants certain rights to individuals as citizens but also entails giving up certain rights to the government.").

78. *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 81–84 (2010); Helen Nissenbaum, *Privacy as a Contextual Integrity*, 79 WASH. L. REV. 119, 125–27 (2004); Helen Nissenbaum, *Securing Trust Online: Wisdom or Oxymoron?*, 81 B.U. L. REV. 635, 635–37 (2001).

79. *See, e.g.*, Richards, *The Dangers of Surveillance*, *supra* note 44, at 1949.

80. *See, e.g.*, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

81. *See, e.g.*, SOLOVE, UNDERSTANDING PRIVACY, *supra* note 62, at 89–100.

82. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 25–26 (1967); Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 11–12 (2013); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1212–20 (1998); Alan F. Westin, *Social and Political Dimensions of Privacy*, 59 J. SOC. ISSUES 1, 3 (2003) ("Every society sets a distinctive balance between the private sphere and the public order, based on the society's political philosophy."); David Pozen, *Privacy-Privacy Tradeoffs*, U. CHI. L. REV. (forthcoming), *available at* http://ssrn.com/abstract=2624281.

83. Increasingly, privacy scholars are framing privacy rights as public goods or collective goods. *See, e.g.*, PRIVACY, DUE PROCESS AND THE COMPUTATIONAL TURN, *supra* note 48, at 17 (in a section titled "Privacy and due process: a search for the public goods that inform the legal rights," Katja de Vries explains that "[t]he right to due process . . . and the right to privacy . . . are not simply moral imperatives or philosophical concepts but fully fledged legal rights that can be derived from a variety of [constitutional] provisions") (citations omitted); PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 221 (1995) (arguing that "privacy serves not just individual interests but common, public, and collective purposes"); Joshua A.T. Fairfield, *Privacy as a Public Good*, DUKE L.J. (forthcoming). Under this theory, the protection of privacy could be conceived as similar to the protection of water and the environment.

Hildebrandt and Katja de Vries encourage an exploration of privacy and due process not "from the perspective of detailed research into positive law, but rather understand them as public goods that inform the legal, moral and political framework of constitutional democracy."[84]

Because the effect of the invisible big data revolution of governance is systemic, the benefit of a method of collective analysis is needed. Procedural due process alone will not recognize or vindicate a right to be free from the type of mass interference or obstruction of access to rights and freedoms that is possible through the government's application of big data technologies. Such a right depends on a definition by which big data blacklisting systems, and the nature and degree of the harm that may result from such systems, can be sorted and assessed. A lack of transparency and a lack of known consequences of these systems complicate defining and characterizing big data blacklisting programs. These systems, many in their infancy, are often classified, semi-classified, or highly bureaucratized and technologically complex. To best recognize big data blacklisting harms, however, it is important to note that big data blacklisting programs may be suspect where they implicate the following:

(1) *Emerging Big Data Governance Tools and Methods*: Establishment of governmental programs and systems that support big data administrative decision-making processes[85] dependent upon "unthinkably large" volumes of data[86] and enormous databases[87] at the disposal of the government to index, catalogue, and analyze individuals for identity and risk-based assessments;[88]

Michael Froomkin provocatively suggests that what he terms "privacy pollution" can be analogized to environmental pollution. A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution*: *Learning from Environmental Impact Statements*, ILL. L. REV. (forthcoming) (manuscript at 1–4), *available at* http://ssrn.com/abstract=2400736.

84. PRIVACY, DUE PROCESS AND THE COMPUTATIONAL TURN, *supra* note 48, at 2.

85. *See, e.g.*, Citron, *Technological Due Process*, *supra* note 28, at 1252 ("The twenty-first century's automated decision-making systems bring radical change to the administrative state that last century's procedural structures cannot manage. In the past, computer systems helped humans apply rules to individual cases. Now, automated systems have become the primary decision makers . . . [and] often take human decision making out of the process[.]") (citations omitted).

86. MAYER-SCHÖNBERGER & CUKIER, *supra* note 2, at 157 ("When the collection expands to information like financial transactions, health records, and Facebook status updates, the quantity being gleaned is unthinkably large.").

87. *Id.*; *see also* GARFINKEL, *supra* note 9, at 54; KUHN, *supra* note 9, at 2–3; Paul Ohm, *Don't Build a Database of Ruin*, HARV. BUS. REV. (Aug. 23, 2012), https://hbr.org/2012/08/dont-build-a-database-of-ruin.

88. *See* Balkin, *supra* note 37, at 12 ("Much public and private surveillance occurs without any knowledge that one is watched. More to the point, data mining technologies allow the state and business enterprises to record perfectly innocent behavior that no one is particularly ashamed of and draw surprisingly powerful inferences about people's behavior, beliefs, and attitudes.").

(2) *Unprecedented Asymmetric Power*: Unprecedented governmental access to public and private data[89] leads to an unprecedented asymmetric power between the state and citizen,[90] facilitated through big data systems and philosophies of governance.[91] These power asymmetries are particularly acute when national security imperatives heighten governmental power[92] while the administrative state objectives may weaken the position of the citizen in relationship to the government,[93] thus necessarily leading to a renegotiation of the "social contract";[94]

(3) *Targeting Suspicious Data, Not People*: Big data technologies facilitate the government's ability to search for suspicious data. Therefore, newly emerging big data programs allow for the tracking and isolation of digitally generated data deemed suspicious, including associational data,[95] correlative data, data patterns, and record location and algorithmically matched data, for instance. The government may use suspicious data and suspicious database screening results to justify a range of consequences suffered by the person attached to the suspicious

89. *See* Balkin & Levinson, *supra* note 37, at 523 (explaining that "information [is] ever more valuable to governments; this causes governments to invest even more heavily in the collection, storage, and collation of data").

90. *See id.*

91. *See* Balkin, *supra* note 37, at 10–11 ("Governance in the National Surveillance State is increasingly statistically oriented, *ex ante* and preventative, rather than focused on deterrence and *ex post* prosecution of individual wrongdoing.").

92. Balkin & Levinson, *supra* note 37, at 523 ("Increased use of information in governance makes governments and those who control information flows more powerful . . . ."); s*ee also* Shirin Sinnar, *Institutionalizing Rights in the National Security Executive*, 50 HARV. C.R.-C.L. L. REV. 289, 346–47 (2015) ("Given the dominance of the security frame, even an interest in rights promotion may lead institutions to explain, justify, and promote rights by appealing to security."); Ernest A. Young, *Welcome to the Dark Side: Liberals Rediscover Federalism in the Wake of the War on Terror*, 69 BROOK. L. REV. 1277, 1284–85 (2004) ("But our modern preoccupation with rights provisions may have encouraged us to overlook the possibility that structure remains a *necessary* condition for liberty. Especially in times of terror, rights provisions may become 'parchment barriers' to governmental oppression. Sometimes it takes a government to check a government.") (citations omitted).

93. Balkin & Levinson, *supra* note 37, at 524–25.

94. *See, e.g.*, CHESTERMAN, *supra* note 52, at 248–52 (2011) (explaining that surveillance technologies are forcing an evolution of the social contract that "differs from the traditional social contract," and observing that "[p]rivacy theorists and lawyers have struggled to respond to these moves, in part because of the diminishing sphere of truly private activity and the growing coercive powers of the state"); *see also* WITTES & BLUM, *supra* note 51, at 13–14.

95. *See* Balkin, *supra* note 37, at 12 ("Data mining allows inferences not only about the direct subjects of surveillance, but about *other people* with whom they live, work, and communicate.") (citing Siobhan Gorman, *NSA's Domestic Spying Grows as Agency Sweeps up Data*, WALL ST. J., Mar. 10, 2008, at A1; James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1464–68 (2004)); Deven Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579, 619–24 (2014).

digitally derived data (e.g., suspicious, Social Security Number (SSN) or metadata from a smartphone).[96] Yet, big data-derived knowledge is unlike small data-derived knowledge in that it is based upon artificial intelligence, allowing some to compare algorithmic-driven determinations to virtual reality;[97]

(4) *Diminishing Transaction Costs*: As a byproduct of the big data revolution, the transaction costs for the collection and analysis of data have rapidly decreased.[98] Therefore, economic restraints on investigatory and administrative capacity to impose consequences are rapidly decreasing as well, especially with the rise of automated or semi-automated processes that can be conducted in real time and remotely, and can be delegated to other private and public entities.[99] Not only are the transaction costs of big data governance rapidly diminishing (e.g., collection and analysis of digital data for "voter integrity" objectives are almost costless), correspondingly, the transaction costs of digitally driven deprivations are rapidly diminishing as well (e.g., big data voter purges that are database-driven are relatively costless compared with small data voter purges);

(5) Ex Ante *and Preventive or Precrime Objectives*: Deployment of big data programs that may often attempt to achieve *ex ante* objectives[100]—including preventive justice or precrime determinations from digital watchlisting and database screening programs—can lead to a range of *ex ante* harms, including the mediation, interference, and obstruction of freedoms and privileges; stigmatization and reputational

96. *See, e.g.*, Cate, *supra* note 37; Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 HARV. J. L. & TECH. 319, 343–48 (2002).

97. *See, e.g.*, Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, *supra* note 30, at 790.

98. Balkin & Levinson, *supra* note 37, at 523 (observing that governance in the National Surveillance State is "spurred on by technological advances that increasingly lower the cost of telecommunications, surveillance technology, data storage, and computation power").

99. Multiple experts have documented the rising corporatization and private delegation of intelligence activities after 9/11. *See, e.g.*, PRIEST & ARKIN, *supra* note 31, at 178–86; HARRIS, THE WATCHERS, *supra* note 31, at 194–98; O'HARROW, *supra* note 31, at 98–107. Big data technologies have also increased the incentives for this private delegation. *See, e.g.*, Lyon, *supra* note 44, at 9 ("Big Data is currently dominated by commercial and governmental criteria[.] . . . Big Data is the strong affinity between the two, particularly in relation to surveillance. Big Data represents a confluence of commercial and governmental interests."); Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, *supra* note 30, at 817–18 (asserting that datafication through big data technologies "[c]an also be understood as the underlying drive to force the issue and reinforce the underlying values of big data: a policy impetus currently underway that mandates or delegates, often under law or administrative regulation, the collection or sharing of more and more data").

100. *See supra* notes 46–49.

costs; restriction of expression, assembly, travel, association, and petition rights; deprivations; and other administrative actions;[101]

(6) *"Guilty Until Proven Innocent" Status*: Big data programs may facilitate a presumption of guilt when an individual is attached to suspicious digital data or database screening results, and may implicitly shift the burden of proof to those who are digitally blacklisted. The mediation of rights, freedoms, and privileges through largely binary and probabilistic big data determinations[102] and the inferences of suspicion[103] that inform big data blacklisting programs are inconsistent with the presumption of innocence necessary to the principle of liberty. Every right and privilege is thus affected and at risk of encumbrance. In effect, the government may be able to precondition both innocence and liberty upon technological processes by prescribing the criteria and consequences for database screening or digital watchlisting systems that inform a big data blacklisting program. Without a presumption of innocence, there is no presumption of liberty;[104]

(7) *"Black Box" Problem*: In a "Black Box Society,"[105] often there is a lack of meaningful notice of the full consequences of the big data

---

101. Cole, *supra* note 1, at 518. Cole observes that a "paradigm of prevention" and *ex ante* determinations or preventive policy can pose a significant threat to liberty interests generally:

> Notwithstanding the ubiquity of preventive motives in ordinary criminal law enforcement, preventive coercion imposed without a specific criminal act poses distinct normative concerns. When the state acts on the basis of predictions, it must necessarily reduce the degree of certainty it demands before imposing coercion, because there is an inherent uncertainty about the future. To the extent that it restricts an individual's liberty based on fear of what she might do in the future, it disrespects her free will to choose to conform her actions to the law.

102. MAYER-SCHÖNBERGER & CUKIER, *supra* note 2, at 78 (observing the distinction between "datafication" and digitization, explaining digitization as "the process of converting analog information into the zeros and ones of binary code so computers can handle it," and datafication "is to put it in a quantified format so it can be tabulated and analyzed").

103. *See id.* at 157 ("[B]ecause the government never knows whom it will want to scrutinize, it collects, stores, or ensures access to information not necessarily to monitor everyone at all times, but so that when someone falls under suspicion, the authorities can immediately investigate rather than having to start gathering the info from scratch."). *See also* Lyon, *supra* note 44, at 10 (observing that "time-honored commitments to the presumption of innocence, or proof beyond a reasonable doubt are eroded" when big data surveillance is combined with a "'penal populism' that calls for public protection, reinforced by media-enhanced perceptions of risk") (citing LUCIA ZEDNER, SECURITY 80 (2009)).

104. *Id.* at 162 ("The fundamental trouble is that with such a system we essentially punish people *before* they do something bad . . . . This negates the very idea of the presumption of innocence, the principle upon which our legal system, as well as our sense of fairness, is based.").

105. PASQUALE, *supra* note 13, at 3. Pasquale states that the "term 'black box' is a useful metaphor . . . given its own dual meaning." The first meaning is that of a "recording device." The second meaning refers to "a system whose workings are mysterious; we can observe its inputs

blacklisting harm and often a lack of access to the full evidence of how one came to be digitally blacklisted (e.g., inability to interrogate algorithms and databases informing big data blacklisting may be classified). Often processes still appear to be small data in nature because the big data elements may be obscured;

(8) *"Everyone is a Potential Target"*:[106] Even with technical notice and minimal remedial procedures, the government may digitally blacklist anyone with a digital trail or a presence within a database, thus harming individuals in ways that may be impossible or impracticable to fully detect and understand;

(9) *Small Data Constitution v. Big Data Constitution*: Preexisting constitutional protections and rights were forged in a small data world to protect against small data harms with small data governing ambitions in mind. Small data limitations on power were presupposed. The current jurisprudence does not impose limiting principles on big data governing ambitions or big data harms that are massive in scope and digitally derived in nature; and

(10) *Largely Invisible Systemic Harms That Are Digitally Derived or Facilitated Yet Difficult to Remediate Technologically*: Big data policy making and programmatic structures have the capacity to lead to a broad range of digitally derived or digitally facilitated systemic harms that can implicate multiple freedoms and privileges. Through the technological mediation and interference of freedoms and privileges—utilizing technologies that may be largely invisible to the common individual—potential consequences may include the chilling of expressive and associational freedoms, infringing upon individual decision-making and autonomy interests, and inalienable rights associated with fundamental liberty interests as broadly construed within the due process framework of protections. At the same time, technological or procedural remedies may be unable to redress these harms, for example, because of the inherent limitations of big data and because of the way in which big data blacklisting programs may lend legitimacy (e.g., the algorithmic-driven "predictive judgments" of the science that informs big data may appear to support a "reasonable suspicion") to inherently illegitimate and

---

and outputs, but we cannot tell how one becomes the other." *Id.*; *see also id.* at 6–8 ("Deconstructing the black boxes of Big Data isn't easy . . . . It matters because authority is increasingly expressed algorithmically."); Citron & Pasquale, *The Scored Society*, *supra* note 13, at 33 ("Opening up the black box scoring systems to individuals or neutral experts representing them is key to permitting them to challenge 'arbitrariness by algorithm.'").

106. *See, e.g.*, James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED, Mar. 15, 2012, http://www.wired.com/2012/03/ff_nsadatacenter ("[A]ccording to [one intelligence] official: 'Everybody's a target; everybody with [digital] communication is a target.'").

unconstitutional outcomes (e.g., deprivation or infringement of fundamental liberty and equality guarantees absent adequate constitutional protections).[107]

II. DATABASE SCREENING AND DIGITAL WATCHLISTING SYSTEMS

Through big data tools, "blacklisting" consequences can be imposed by the government absent an actual "blacklist" or even a "list" of names. Unlike the manner in which "blacklisting" practices unfolded in a small data world, an overview of the mechanics of potential big data blacklisting programs demonstrates that the harms of inferential guilt can flow from digitally generated data. Thus, many of the big data blacklisting programs discussed below are not necessarily comprised of a list of individuals who have been placed on a "blacklist" for government consequences. Rather, these programs utilize big data tools to access and analyze digital data or databases. Once this data is accessed and analyzed, the big data tools can be used deliberately or inadvertently to flag the digitally suspicious. Thus, big data blacklisting programs may, but do not necessarily, draw up a list of individuals for deprivation purposes. The database screening and digital watchlisting systems discussed below show that it is often digitalized data deemed guilty and suspicious that is flagged by the big data tools, and it is not necessarily guilty or suspicious persons who are flagged.

Because many of these programs are classified or semi-classified, it is unclear exactly what digital data or databases, and what statistical analytical methods or algorithmic tools, the government engages to determine how to assess the "guilt" of those targeted by these big data programs. Yet, these programs may facilitate the assessment of a "guilty until proven innocent" status.[108] To illustrate the new pressures that have been placed on the existing due process jurisprudence in challenging these big data programs, Part II describes the mechanics of various government programs that rely upon big data tools. By necessity, a careful description of these programs is a highly technical undertaking. A close examination of the big data technologies and the administrative systems that support their consequences, however, is required in order to more fully appreciate the constitutional harms that may attach to these big data blacklisting programs.

These database screening and digital watchlisting systems, for example, include nonclassified programs—such as the No Work List

107. *See* Daskal, *supra* note 33, at 362 ("[P]re-crime restraints also interfere with the important liberty interest in being treated with equal dignity.").

108. LYON, *supra* note 32, at 185 ("[U]sing personal data analysis and algorithms . . . the potential offender, is singled out for attention by virtue of being identified as part of a group with certain characteristics . . . the goal is to attach suspicion, perhaps leading to a criminal charge.") (citations omitted).

(e.,g., E-Verify), the No Vote List (e.g., SAVE, HAVA, etc.), and the No Citizenship List (e.g., S-COMM/PEP, etc.)—and classified or semi-classified programs—such as the No Fly List and the Terrorist Watchlist. In the discussion below, it is important to recognize, however, that the big data technologies (e.g., E-Verify and HAVA) discussed here are simply representative technologies. SAVE/HAVA database screening is not coterminous with the "No Vote List" per se. The technologies are rapidly evolving. Multiple big data tools that may potentially disenfranchise voters will not be discussed below (e.g., Interstate Crosscheck [database screening] Program is not discussed below, however, some may argue that it is a "No Vote List").[109] The specific database screening systems that are deployed today may not be deployed in the future. Thus, the focus of the inquiry in this Article is a constitutional one, for instance, how a big data-driven "No Vote List" database screening system may impact fundamental liberty interests.

Finally, it is worth noting that technologies and programs that once were not considered "big data" in a small data world (e.g., computerized identity data matching systems) have now been transformed in a big data world (e.g., big data mass integration systems using complex algorithmic tools to conduct identity verification).[110] The E-Verify database screening system, for example, was recently identified as a "big data" program in the White House's report *Big Data: Seizing Opportunities, Preserving Values*.[111] In a small data world, this program may not have appeared to be sufficiently "big data"-oriented to qualify as a big data program.

A. *Nonclassified Big Data Programs*

Core constitutional rights and freedoms in a small data world may, in the National Surveillance State,[112] fare differently from rights and freedoms in a big data world.[113] A small data world is free of massive

109. *See, e.g.*, KRIS W. KOBACH, NAT'L ASS'N OF STATE ELECTION DIRS., INTERSTATE VOTER REGISTRATION CROSSCHECK PROGRAM (2013), *available at* http://www.nased.org/NASED_Winter_2013_PP_Presentations/KANSAS.pdf.

110. *See, e.g.*, Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1489–99 (2013) (discussing the functionality of various identity verification and identity determination systems through a biometric ID cybersurveillance structure).

111. PODESTA REPORT, *supra* note 6, at 52–53 (discussing concerns surrounding E-Verify).

112. Balkin explains that the "National Surveillance State" necessarily impacts core rights and freedoms, as the digital age has ushered in a "new form of governance" that harnesses information technologies to serve governmental goals. Balkin, *supra* note 37, at 3 ("This new form of governance is the National Surveillance State. In the National Surveillance State, the government uses surveillance, data collection, collation, and analysis to identify problems, to head off potential threats, to govern populations, and to deliver valuable social services.").

113. The appropriate uses of dataveillance and cybersurveillance in determining public policy choices—and the legality and constitutionality of these emerging data-driven

databases, invisible dataveillance and cybersurveillance systems, and automated or semi-automated data screening programs. In a small data world, individuals take for granted the ability to live freely and access fundamental liberty interests directly without digital mediation or technological obstruction. In a small data world, a citizen can exercise a constitutional right or freedom without database screening, digital data analysis, or other technological interference by the government or its delegates.[114]

In contrast, in a big data world, the government can digitally mediate—and consequently threaten—privileges, rights, liberty interests, and freedoms.[115] The processes in which fundamental rights can be deprived in a small data world are radically different from the processes in which fundamental rights can be deprived in a big data world. In a big data world, government analysis and decision-making processes can unfold virtually and invisibly,[116] for instance, through data screening systems. The government may gather data-driven evidence to determine guilt in an administrative manner, often embedded within a highly bureaucratized structure,[117] in a way that is almost impossible to contest.

The right to work and vote, for example, are rights many citizens perceive as fundamental. The discussion below describes how the government and its delegates can utilize big data screening tools and database-driven, risk-based assessments to impair work opportunities, deny the right to vote, and abridge the rights and privileges of citizenship.

1. No Work List

The E-Verify program, jointly operated by the U.S. Department of Homeland Security (DHS) and the Social Security Administration (SSA),

---

technologies—have informed the work of multiple experts in recent years. *See generally, e.g.*, MAYER-SCHÖNBERGER & CUKIER, *supra* note 2, at 8–9; MOROZOV, *supra* note 40; Kerr, *Fourth Amendment and New Technologies*, *supra* note 55, at 802–08; Omer Tene, *Big Data for All: Privacy and User Control*, STAN. L., CTR. FOR INTERNET & SOC'Y (Sept. 20, 2012, 4:05 PM), http://cyberlaw.stanford.edu/blog/2012/09/big-data-all-privacy-and-user-control-age-analytics.

114. *See, e.g.*, Citron, *Technological Due Process*, *supra* note 28, at 1281; Daniel J. Solove, *Digital Dossiers*, *supra* note 8, at 1107 & n.130 ("[B]y obtaining private sector records, the government can conduct the type of 'fishing expeditions' that the Framers feared.").

115. *See, e.g.*, Balkin, *supra* note 37, at 12; Balkin & Levinson, *supra* note 37, at 490; Wittes, *supra* note 57, at 2.

116. *See* Balkin, *supra* note 37, at 12.

117. LYON, *supra* note 32, 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"); *see also* SOLOVE, DIGITAL PERSON, *supra* note 39, at 13–21 (describing the manner in which modern privacy violations occur as a result of corporate and bureaucratic action).

is referred to as the "No Work List" in various outlets.[118] E-Verify is similar to the No Fly List in its adverse impact on U.S. citizens and lawful immigrants.[119] Critics of E-Verify claim that the database screening system has wrongly disenfranchised individuals of the opportunity to work in a similar manner that the critics of the No Fly List claim the digital watchlisting system has wrongly disenfranchised citizens of the opportunity to fly.[120]

E-Verify is an Internet-based identity verification system[121] that relies upon database screening protocols.[122] The E-Verify system attempts to "verify" the identity or citizenship status of a worker based upon complex statistical algorithms and multiple databases.[123] Put into simple terms: First, an enrolled employer collects personally identifiable data from an employee—e.g., the employee's name, date of birth, photo identification, and SSN.[124] Next, that employer (or its designated agent) enters the gathered information into either the web service or browser based software system.[125] The data is matched to the SSA database and various DHS immigration databases to determine whether the employee may legally work.[126]

---

118. *See, e.g.*, Press Release, ACLU, Employment Verification Would Create a 'No Work List' in the United States (May 6, 2008), https://www.aclu.org/immigrants-rights/employment-verification-would-create-'no-work-list'-us; Jim Harper, *Immigration Reform: REAL ID and a Federal 'No Work' List*, CATO INST. (June 14, 2007), http://www.cato.org/publications/techknowledge/immigration-reform-real-id-federal-no-work-list. For an overview of the E-Verify program and some of its legal implications, see generally Stumpf, *Getting to Work*, *supra* note 16 (outlining the procedures and policies of E-Verify).

119. *See* Harper, *supra* note 118.

120. *See, e.g.*, *id.*

121. Identity verification systems seek to confirm or authenticate identity data presented by an individual, checking produced data against an existing database. *See, e.g.*, JENNIFER LYNCH, FROM FINGERPRINTS TO DNA: BIOMETRIC DATA COLLECTION IN U.S. IMMIGRANT COMMUNITIES AND BEYOND 5 (2012).

122. WESTAT, WESTAT EVALUATION OF THE E-VERIFY PROGRAM: USCIS SYNOPSIS OF KEY FINDINGS AND PROGRAM IMPLICATIONS 1 (2010) [hereinafter WESTAT, EVALUATION OF E-VERIFY], *available at* http://www.uscis.gov/USCIS/Native%20Docs/Westat%20Evaluation%20of%20the%20E-Verify%20Program.pdf.

123. *See E-Verify: Preserving Jobs for American Workers*, *Hearing Before the Subcomm. on Immigration Policy & Enforcement of the H. Comm. on the Judiciary*, 112th Cong. 34–35 (2011) (statement of Theresa C. Bertucci, Assoc. Dir., Enter. Servs. Directorate, U.S. Citizenship & Immigration Servs.); WESTAT, EVALUATION OF E-VERIFY, *supra* note 122, at 1, 5.

124. *See* U.S. CITIZENSHIP & IMMIGRATION SERVS., I AM AN EMPLOYER: HOW DO I USE E-VERIFY? 1–2 (2013), *available at* http://www.uscis.gov/USCIS/Resources/E4en.pdf.

125. *Id.* at 1.

126. SSA maintains the Numerical Identification File (NUMIDENT) SSN database, which includes the name, date of birth, and other biographical information of SSA applicants. ANDORRA BRUNO, CONG. RESEARCH SERV., R40446, ELECTRONIC EMPLOYMENT ELIGIBILITY VERIFICATION 2 (2009). The United States Citizenship and Immigration Services (USCIS) maintains the Verification Information System (VIS) database, which "is comprised of citizenship,

Generally, the results of the inquiry are returned to the employer within seconds, and the employee's identity is either "verified"[127] or "not verified." If there is an anomalous result from the database screening algorithms, the employee falls into a category referred to as "Tentative Nonconfirmation" (TNC).[128] Upon a TNC result, the employer is required to allow the employee to contest the finding.[129] It is the responsibility of the employee to contact DHS or SSA "within 8 federal government workdays to correct the TNC."[130] If the TNC remains unresolved, the system generates a "Final Nonconfirmation" (FNC) finding.[131] If an employee does not contact DHS or SSA, the system generates a "No Show" result after ten business days have passed.[132] An employer can terminate an employee after the employee receives either a "No Show" or FNC result.[133]

If DHS concludes that the employee did not take sufficient steps to correct the mismatch, and if the E-Verify system issues a FNC to the employer, then there is no formal process to contest or appeal such a determination.[134] For those employees who have affirmatively elected to contest the TNC through signing an E-Verify form generated by the E-

---

immigration, and employment status information from several DHS System of Records." 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.

127. *The Verification Process*, U.S. DEP'T OF HOMELAND SEC., U.S. CITIZENSHIP & IMMIGRATION SERVS., http://www.uscis.gov/e-verify/employers/verification-process (last visited Oct. 16, 2015).

128. *Id.*

129. *Employee Rights and Responsibilities*, U.S. CITIZENSHIP & IMMIGRATION SERVS., http://www.uscis.gov/e-verify/employees/employee-rights-and-responsibilities (last visited Oct. 16, 2015).

130. *How to Correct a Tentative Nonconfirmation*, U.S. CITIZENSHIP & IMMIGRATION SERVS., http://www.uscis.gov/e-verify/employees/how-correct-tentative-nonconfirmation (last visited Oct. 16, 2015).

131. *DHS TNCs*, U.S. CITIZENSHIP & IMMIGRATION SERVS., http://www.uscis.gov/e-verify/employers/tentative-nonconfirmations/dhs-tncs (last visited Oct. 16, 2015); *see also* DEP'T OF HOMELAND SEC., THE E-VERIFY MEMORANDUM OF UNDERSTANDING FOR EMPLOYERS (2013) [hereinafter DEP'T OF HOMELAND SEC., E-VERIFY EMPLOYMENT VERIFICATION MEMORANDUM], *available at* http://www.uscis.gov/site/default/files/USCIS/Verification/E-Verify/E-Verify_Native_Documents/MOU_for_E-Verify_Employer.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.").

132. *DHS TNCs*, *supra* note 131.

133. *Id.*

134. John Fay, *USCIS Considers Secondary Review Process for E-Verify Final Nonconfirmations*, LAWLOGIX (Feb. 13, 2012), http://www.lawlogix.com/blog/uscis-considers-secondary-review-process-e-verify-final-nonconfirmations.

Verify system, the federal government is then provided two days after the original eight business days have passed (for a total of ten business days) to make a manual determination as to the individual's work authorization.[135]

Despite significant challenges faced by the program thus far, E-Verify is poised for mandatory national expansion. At the federal level, E-Verify is a voluntary pilot program.[136] Yet, multiple state laws have begun to mandate that employers within their state use the system. [137] In *Chamber of Commerce v. Whiting*, the Supreme Court upheld the Legal Arizona Workers Act,[138] which requires all employers in Arizona to run all new worker's information through the E-Verify program.[139]

Past and current legislative proposals recommend the national, mandatory expansion of E-Verify, for example through the New Employee Verification Act[140] and proposed comprehensive immigration reform bills, including the Bipartisan Senate Immigration Plan introduced in April 2013, titled Border Security, Economic Opportunity, and Immigration Modernization Act.[141] Further, it is significant to note that E-Verify use is rapidly expanding. As of September 2015, over 600,000

135. DEP'T OF HOMELAND SEC., E-VERIFY EMPLOYMENT VERIFICATION MEMORANDUM, *supra* note 131, at 9. The manual determination can include putting a case in continuance if more time is necessary, for example, if the employee has applied for and is waiting on a replacement document. *See DHS TNCs*, *supra* note 131.

136. 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." (internal quotation marks omitted)). Congress expressly prohibited DHS from requiring private employers to use E-Verify on anything other than a voluntary basis. *See* IIRIRA, Pub. L. No. 104-208, § 402, 110 Stat. 3009–546 (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' E-Verify." (quoting IIRIRA § 402(a), (e))).

137. *See, e.g.*, Hu, *Reverse-Commandeering*, *supra* note 16, 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)).

138. ARIZ. REV. STAT. ANN. §§ 23-211 to -216 (2015) (prohibiting employers from knowingly hiring an "unauthorized alien").

139. *Whiting*, 131 S. Ct. at 1972, 1985 (holding that an Arizona immigration statute requiring employers engage in mandatory E-Verify database screening is not preempted by federal immigration law because federal law only prohibits the federal government from mandating E-Verify, and nothing in the federal law prohibits states from mandating E-Verify); *see also* Hu, *Reverse-Commandeering*, *supra* note 16, at 598–99.

140. H.R. 2028, 111th Cong. § 103 (1st Sess. 2009).

141. S. 744, 113th Cong. § 3 (1st Sess. 2013).

employers use E-Verify at more than 1.4 million hiring sites to screen new hires over the Internet.[142] Approximately 1400 new companies join this pilot program per week.[143] The 52 million U.S. workers hired in 2012 were subjected to approximately 21.2 million queries in the E-Verify system.[144]

2. No Vote List

Immediately following the Supreme Court's June 2013 ruling in *Shelby County v. Holder*[145] that struck down Section 4(b) of the Voting Rights Act of 1965,[146] multiple states announced their intention to remove noncitizens from voter registration rolls through a database screening system referred to as the SAVE database. DHS maintains and operates the SAVE database.[147] Since the creation of SAVE through the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA),[148] SAVE has provided benefits-granting agencies at the federal, state, and local level with a method to verify eligibility for

142. *What Is E-Verify?*, U.S. CITIZENSHIP & IMMIGR. SERVS., http://www.uscis.gov/e-verify/what-e-verify (last updated June 25, 2015).

143. *Id.*

144. Alex Nowrasteh, *CATO FOIA Request Reveals E-Verify Delays Hurt Workers*, CATO INST. (Jan. 17, 2014, 12:16 PM), http://www.cato.org/blog/cato-foia-request-reveals-e-verify-delays-hurt-workers.

145. Shelby Cnty. v. Holder, 133 S. Ct. 2612, 2631 (2013) (holding that the Voting Rights Act's federal preclearance formula for state election procedures as unconstitutional under the Tenth Amendment). Multiple scholars have investigated the constitutional and other legal implications of the Voting Rights Act immediately preceding and after the decision in *Shelby County*. *See, e.g.*, Samuel R. Bagenstos, *Universalism and Civil Rights (with Notes on Voting Rights After* Shelby*)*, 123 YALE L.J. 2838, 2841–42 (2014) (arguing that "the response to Shelby County will fail unless it goes well beyond universal protections of voting rights[,]" and that "the voting rights regime must also provide robust protection against race discrimination specifically"); Guy-Uriel E. Charles & Luis Fuentes-Rohwer, *State's Rights*, *Last Rites, and Voting Rights*, 47 CONN. L. REV. 481, 485–86 (2014) (arguing that *Shelby County* should be viewed "as deeply destabilizing to the infrastructure of voting rights law and policy[,]" and undermines the "basic assumptions" that have traditionally included: the "primacy" of "the federal government over the states with respect to the authority to regulate elections[,]" "accord[ing] Congress a fair amount of deference" in addressing "racial discrimination in democratic politics[,]" and the three branches "have generally operated from a similar and fluid conception of racial discrimination"); Samuel Issacharoff, *Beyond the Discrimination Model on Voting*, 127 HARV. L. REV. 95, 121 (2013) (proposing a regulatory approach that requires a disclosure system involving a "voting impact statement" of the "likely anticipated effect on access to the ballot and any known anticipated impact on minority voters in particular").

146. *Shelby Cnty.*, 133 S. Ct. at 2631.

147. *What Is SAVE?*, U.S. DEP'T OF HOMELAND SEC., U.S. CITIZENSHIP & IMMIGRATION SERVS., http://www.uscis.gov/save/what-save/what-save (last visited Oct. 16, 2015).

148. IIRIRA, Pub. L. No. 104-208, 110 Stat. 3009-546 (codified in scattered sections of 8 U.S.C. and 18 U.S.C.).

government aid programs, such as Medicaid, through identity and immigration alien number database screening.[149]

In July 2012, one month after the U.S. Supreme Court issued *Shelby County*, thirteen states led by Colorado petitioned DHS for access to its SAVE database screening protocols for the purpose of identifying possible noncitizens to purge from voter rolls.[150] Specifically, DHS informed a federal district court that Florida would have access to the SAVE database screening system.[151] Shortly thereafter, DHS entered into a Memorandum of Agreement (MOA) with Florida permitting it access to SAVE for the purposes of verifying its voter registration rolls.[152] In August 2012, DHS entered into a similar MOA with Colorado.[153]

Florida and Colorado utilize the SAVE database by first drawing upon immigration-related information provided by each state's Department of Motor Vehicles (DMV).[154] Next, the state election official compares the names of noncitizens in DMV records to the names of registered voters.[155] State election officials purge individuals from the voter registration polls by determining if a voter failed to gain citizenship after obtaining a driver's license (e.g., if the voter remains in the SAVE database as an immigrant).[156] Under SAVE, an Internet-based query searches over 100 million records contained in DHS databases.[157] The database screening protocol attempts to determine if there is a match between the personally identifiable data entered into the database screening system and DHS records on an individual's immigration status.[158]

149. *See, e.g.*, Omnibus Consolidated Appropriations Act, 1997 § 404, Pub. L. No. 104-208, 110 Stat. 3009.

150. *See* Letter from Scott Gessler, Colo. Sec'y of State, to Janet Napolitano, U.S. Sec'y of Homeland Sec. (July 9, 2012), *available at* http://www.scribd.com/doc/99815699/SOS-Sec-Napolitano-Ltr-7-9-12-FINAL.

151. *See* Charles Babington, *AP Newsbreak: In Victory for GOP, Florida Wins Access to Homeland Security List of Noncitizens*, ASSOCIATED PRESS (July 14, 2012, 8:17 PM), *available at* http://m.startribune.com/nation/162465396.html; Letter from Alejandro Mayorkas, U.S. Citizenship & Immigration Servs. Dir., to Ken Detzner, Fla. Sec'y of State (June 12, 2012), *available at* http://bradblog.com/Docs/USCIS_Mayorkas_LetterTo_FLDetzner_061212.pdf.

152. Memorandum of Agreement Between the Dep't of Homeland Sec., U.S. Citizenship & Immigration Servs., and Fla. Dep't of State, Div. of Elections (Aug. 14, 2012), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/805148/moa-dhs-fl-1.pdf; *see also* Corey Dade, *States to Use U.S. Immigration List for Voter Purges*, NPR (July 17, 2012, 3:51 PM), http://www.npr.org/2012/07/17/156880856/states-to-use-u-s-immigration-list-for-voter-purges.

153. Memorandum of Agreement Between the Dep't Homeland Sec., U.S. Citizenship & Immigration Servs., and Colorado Secretary of State (Aug. 22, 2012).

154. *See, e.g.*, Marouf, *supra* note 17, at 67.

155. *See id.*

156. *See id.* at 67–68.

157. *What is SAVE?*, *supra* note 147.

158. *See id.*

DHS has granted SAVE database screening access to a total of five states for voter registration purges. In addition to Florida and Colorado, three states—Iowa,[159] North Carolina,[160] and Virginia[161]—have entered into an MOA agreement with DHS to access the SAVE database. Five counties in Arizona have also entered into an MOA to use the SAVE database for the same purpose.[162] At least eleven additional states have requested access to the SAVE database for voter purges, including Alaska, Arkansas, Georgia, Kansas, Michigan, Nevada, New Mexico, Ohio, Texas, Utah, and Washington.[163]

In addition to SAVE, state election officials currently conduct database screening protocols pursuant to the HAVA.[164] Per Section 15483(a) of HAVA, each state is required to create and maintain an electronic database that contains all registered voters.[165] States are also required to verify the identity of voter registration applicants by cross checking the last four digits of the applicant's SSN or driver's license.[166] The state agency tasked with overseeing elections and procedures is required by HAVA to coordinate with SSA for SSN database screening purposes.[167] If a prospective voter does not have a SSN or a driver's license, the state must assign a voter ID number to the applicant. Critics of voter purges under SAVE and HAVA note that neither the SAVE database screening system nor the HAVA–SSA database screening

159. Muzaffar Chishti & Faye Hipsman, *State Access to Federal Immigration Data Stirs New Controversy in Debate over Voting Rights*, MIGRATION POLICY INST. (Sept. 12, 2013) http://www.migrationpolicy.org/article/state-access-federal-immigration-data-stirs-new-controversy-debate-over-voting-rights.

160. *Id.*

161. Kara Brandeisky et al., *Everything That's Happened Since Supreme Court Ruled on Voting Rights Act*, PROPUBLICA.ORG (Nov. 4, 2013, 12:31 PM), http://www.propublica.org/article/voting-rights-by-state-map.

162. Chishti & Hipsman, *supra* note 159; *see also Using the Systematic Alien Verification for Entitlements (SAVE) Program for Voter Eligibility Verification*, IMMIGRATION POLICY CTR. (Aug. 2, 2012), http://www.immigrationpolicy.org/just-facts/using-systematic-alien-verification-entitlements-save-program-voter-eligibility-verificat.

163. Chishti & Hipsman, *supra* note 159.

164. HAVA, Pub. L. No. 107-252, 116 Stat. 1666, 1666–730 (2002) (codified as amended at 42 U.S.C. §§ 15301–15545 (2012)).

165. 42 U.S.C. § 15483(a) (2012).

166. *Id.* § 15483(a)(5)(A)(i). The HAVA database screening protocol statutorily requires that state election officials match the voter registration to other database lists with the purported intent to more robustly protect voter integrity. Daniel P. Tokaji, *Voter Registration and Election Reform*, WM. & MARY BILL RTS. J. 453, 478–80 (2008). The protocol does not, however, stipulate how the matches are to be conducted through a database screening system nor does it specify what steps are appropriate once a database match is found. *Id*.

167. *See President Signs HAVA*, *supra* note 18.

system was designed to verify identity or citizenship status for voter registration purposes.[168]

3. No Citizenship List

S-COMM is an interoperability program that facilitates data sharing and database screening protocols between the Federal Bureau of Investigation (FBI), DHS, and local law enforcement agencies.[169] As of 2013, pursuant to a mandate by DHS, S-COMM's database screening protocols were required by all state and local law enforcement agencies.[170] Consequently, after the mandate, what was formerly a pilot program was converted into a mandatory program.[171] The mandatory database screening protocols required state and local law enforcement agencies to run fingerprints collected from suspects against federal fingerprint databases.[172]

Federal courts have expressed Fourth Amendment and other constitutional concerns about detention periods under S-COMM.[173] DHS responded with policy changes to S-COMM in 2014.[174] First, S-COMM

168. *See, e.g.*, Janell Ross, *Voter Roll Purges Could Spread to at Least 12 States*, HUFFINGTON POST (July 31, 2012, 8:01 AM), http://www.huffingtonpost.com/2012/07/31/voter-roll-purge_n_1721192.html.

169. S-COMM commenced as a pilot program in March 2008 under President George W. Bush and was piloted in fourteen jurisdictions by October 2008. AARTI KOHLI ET AL., 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.

170. *See* Kirk Semple & Julia Preston, *Deal to Share Fingerprints Is Dropped, Not Program*, N.Y. TIMES (Aug. 6, 2011), http://www.nytimes.com/2011/08/06/us/06immig.html.

171. In 2010, before the efficacy of the piloted program could be fully assessed, DHS determined that all state and local law enforcement agencies would be required to implement S-COMM by 2013. *See* Memorandum from Riah Ramlogan, Deputy Principal Legal Advisor, on Secure Communities—Mandatory in 2013 to Beth N. Gibson, Assistant Deputy Dir., U.S. Immigration & Customs Enforcement, (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), http://www.nytimes.com/2011/08/13/us/politics/13secure.html.

172. LYNCH, *supra* note 121, at 9.

173. *E.g.*, Miranda-Olivares v. Clackamas Cnty., No. 3:12-cv-02317-ST, 2014 WL 1414305, at *11 (D. Or. Apr. 11, 2014); Morales v. Chadbourne, 996 F. Supp. 2d 19, 28–32 (D.R.I. 2014); *see also* Memorandum from Jeh Charles Johnson, *supra* note 19, at 2 (responding to federal court holdings that "detainer-based detention . . . violates the Fourth Amendment" by directing ICE to "replace requests for *detention* . . . with requests for *notification* (i.e., requests that state or local law enforcement notify ICE of a pending release during the time that person is otherwise in custody under state or local authority).").

174. *See, e.g.*, Juliet P. Stumpf, *D(e)volving Discretion: Lessons from the Life and Times of Secure Communities*, 64 AM. UNIV. L. REV. 1259, 1262 (2015) (describing the policy decisions that led to the "demise" of S-COMM and the adoption of the Priority Enforcement Program (PEP)).

was renamed "Priority Enforcement Program" (PEP).[175] Although DHS stated that the program was "discontinued as we know it," the changes did not appear to impact the database screening protocols of S-COMM.[176] Next, DHS explained that the new program by U.S. Immigration and Customs Enforcement (ICE) impacts detainer requests by limiting enforcement actions: "[U]nless the alien poses a demonstrable risk to national security, enforcement actions through the new program will only be taken against aliens who are convicted of specifically enumerated crimes."[177] However, "ICE . . . will continue to rely on fingerprint-based biometric data submitted during bookings by state and local law enforcement agencies to the [FBI] . . . for criminal background checks."[178]

In short, S-COMM—now the newly renamed PEP—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.[179] Although a gross simplification, S-COMM/PEP database screening works in the following way. Local law enforcement agencies (LEA), upon arresting a suspect, collect and scan the suspect's fingerprints. The LEA submits the fingerprints, and they are checked against the FBI and DHS databases.[180] If the fingerprints match one in the database, the FBI sends an Immigration Alien Query to the Law Enforcement Support Center (LESC). For detention and deportation

175. Memorandum from Jeh Charles Johnson, *supra* note 19, at 3.

176. *Id.* at 1.

177. *Id.* at 2.

178. *Id.*

179. *See* LYNCH, *supra* note 121, at 6–8.

180. The FBI maintains the Integrated Automated Fingerprint Identification System (IAFIS) database. *Integrated Automated Fingerprint Identification System*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited Oct. 16, 2015). DHS maintains the Automated Biometric Identification System (IDENT) database. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT) 2 (2006) [hereinafter U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR IDENT], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf ("IDENT is a Department of Homeland Security (DHS)-wide system for the collection and processing of biometric and limited biographic information for DHS . . . ."). The database screening process can be summarized as follows: "1. . . . [T]he arresting LEA sends the subject's fingerprints and associated biographical information to [Criminal Justice Information Services (CJIS)]/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. DEP'T OF HOMELAND SEC., U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, SECURE COMMUNITIES: QUARTERLY REPORT: FISCAL YEAR 2010 REPORT TO CONGRESS FOURTH QUARTER 2–3 (2011) [hereinafter ICE, SECURE COMMUNITIES: QUARTERLY REPORT], *available at* http://www.ice.gov/doclib/foia/secure_communities/congressionalstatusreportfy104thquarter.pdf.

determinations, multiple databases are researched by the LESC, managed by DHS's ICE.[181]

Multiple 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/PEP.[182] Some of these laws, however, do so in a way that expands the scope of S-COMM/PEP.[183] For instance, in *Arizona v. United States*,[184] the Court upheld § 2(B) of Arizona Senate Bill 1070.[185] This controversial state law was referred to in the media as the "racial profiling" law and the "show me your papers" law.[186] Whereas PEP targets only those individuals "arrested and booked by a law enforcement officer for a criminal violation,"[187] Section 2(B) states that

181. ICE, SECURE COMMUNITIES: QUARTERLY REPORT, *supra* note 180, at 4–5.

182. 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) (2015). For an overview of Section 2(B), see MOTOMURA, *supra* note 20, at 64–65, 113–15, 125–26, 138–39, 151–52; Hu, *supra* note 16, at 596–604. Several scholars have dedicated important research to SB 1070 specifically, and local immigration regulation and immigration federalism, and its implications. *See, e.g.*, Jennifer M. Chacón, *The Transformation of Immigration Federalism*, 21 WM. & MARY BILL RTS. J. 577 (2012); Gabriel J. Chin & Marc L. Miller, *The Unconstitutionality of State Regulation of Immigration Through Criminal Law*, 61 DUKE L.J. 251, 253–54 (2011); Lucas Guttentag, *Immigration Preemption and the Limits of State Power: Reflections on* Arizona v. United States, 9 STAN. J. C.R. & C.L. 1, 7–15 (2013); Jennifer Lee Koh, *Rethinking Removability*, 65 FLA. L. REV. 1803 (2013); Kevin R. Johnson, *Immigration and Civil Rights: State and Local Efforts to Regulate Immigration*, 46 GA. L. REV. 609, 632–35 (2012); David Martin, *Reading* Arizona, 98 VA. L. REV. IN BRIEF 41 (2012); Cristina M. Rodríguez, *The Significance of the Local Immigration Regulation*, 106 MICH. L. REV. 567 (2008); Pratheepan Gulasekaram & Karthick Ramakrishnan, *The President and Immigration Federalism*, 68 FLA. L. REV. (forthcoming 2016).

183. 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) (2012) and mandates this database screening protocol through express incorporation of the federal immigration statute into the language of the state immigration statute.

184. 132 S. Ct. 2492 (2012).

185. ARIZ. REV. STAT. ANN. § 11-1051(B) (2015).

186. *Id.* at 2507–10 (holding that it was improper to enjoin Section 2(B) on preemption grounds because if Section 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").

187. *Priority Enforcement Program*, U.S. DEP'T OF HOMELAND SEC., U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, https://www.ice.gov/pep (last visited Oct. 16, 2015) ("PEP begins at the state and local level when an individual is arrested and booked by a law enforcement officer for a criminal violation and his or her fingerprints are submitted to the FBI for criminal history and warrant checks. This same biometric data is also sent to U.S. Immigration and Customs Enforcement (ICE) so that ICE can determine whether the individual is a priority for removal . . . .").

"where reasonable suspicion exists that the person is an alien who is unlawfully present in the United States, a reasonable attempt shall be made, when practicable, to determine the immigration status of the person."[188]

B. *Classified and Semi-Classified Big Data Programs*

Big data cybersurveillance and dataveillance tools facilitate the government's ability to target those deemed suspicious by virtue of suspect digital data and metadata. Yet, the challenges associated with automated or semi-automated decision-making and algorithmic intelligence through government-led big data systems can be almost impossible to remediate. In other words, the digital mediation of core constitutional rights through big data tools can impact both the manner in which the government administers and justifies the conferral of rights and privileges, and the manner in which the government conducts and justifies the deprivation of rights and privileges.

This problem is particularly acute when the fundamental rights involve the potential deprivation of life and liberty without the due process of law. The constitutional guarantee of due process of law is especially challenged, however, when the government exercises deprivations of life and liberty under classified programs that promote sensitive national security objectives. The discussion below describes how the government can utilize big data screening tools and database-driven, risk-based assessments to justify digital watchlisting and database screening systems to categorize individuals as potential national security threats and to single out these individuals for deprivations, such as the denial of the right to fly.

1. Terrorist Watchlist

After the terrorist attacks of September 11, 2001, in order to administratively formalize terrorist screening and watchlisting, President George W. Bush issued a directive, Homeland Security Presidential Directive 6 (HSPD-6), to the U.S. Department of Justice (DOJ), requiring the "establish[ment of] an organization to consolidate the Government's

188. ARIZ. REV. STAT. ANN. § 11-1051(B) (2015); *see also* Hu, *Reverse-Commandeering*, *supra* note 16, 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.").

approach to terrorist screening."[189] Pursuant to HSPD-6, the DOJ established the Terrorism Screening Center (TSC) as a multi-agency center for coordinating information pertaining to terrorist activity.[190] Then-U.S. Attorney General John Ashcroft established the TSC to oversee FBI-related terrorist data collection and screening.[191] HSPD-6 specifically mandated the development of a TSDB as a consolidated terrorist watchlist maintained by the TSC,[192] combining as many as

189. Homeland Security Presidential Directive/HSPD-6—*Directive on Integration and Use of Screening Information to Protect Against Terrorism*, 39 WEEKLY COMP. PRES. DOC. 1234, 1234 (Sept. 16, 2003) [hereinafter Homeland Security Presidential Directive/HSPD-6], *available at* http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf. The National Counterterrorism Center summarizes the intent of HSPD-6 in the following way:

> The intent of HSPD-6 was to consolidate all TERRORISM INFORMATION at the Terrorist Threat Integration Center (TTIC)—whose functions were assumed by the [National Counterterrorism Center]—in a classified database that would then extract Unclassified, For Official Use Only (U//FOUO) TERRORIST IDENTIFIERS for passage to the new organization created by the Attorney General. Thus, concurrent with the issuance of HSPD-6, the TSC was established via the *Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism* (TSC [Terrorist Screening Center] MOU), which was signed by the Attorney General, the Secretaries of State and Homeland Security, and the Director of Central Intelligence (on behalf of the [Intelligence Community]).

NAT'L COUNTERTERRORISM CTR., WATCHLISTING GUIDANCE 6 (Mar. 2013), *available at* https://firstlook.org/theintercept/document/2014/07/23/march-2013-watchlisting-guidance/.

190. *Id.*

191. According to the FBI, the agency maintains the Terrorist Screening Center as a "24/7 Operations Center . . . and operates the U.S. Government's consolidated Terrorist Screening Database (TSDB), often referred to as the 'Terrorist Watchlist,' and serves as a bridge between law enforcement, Homeland Security, the Intelligence Community, and international partners." *About the Terrorist Screening Center*, FED. BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, *available at* https://www.fbi.gov/about-us/nsb/tsc/about-the-terrorist-screening-center; *see also* Brief of Plaintiffs-Appellants at 5, Latif v. Holder, 686 F.3d 1122 (9th Cir. 2012) (No. 11-35407), *available at* https://www.aclu.org/files/assets/latif_v__holder_brief_of_plaintiffs-appellants_filed.pdf.

192. *See* Homeland Security Presidential Directive/HSPD-6, *supra* note 189. HSPD-6 directs the Attorney General

> to (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information as appropriate and to the full extent permitted by law to support (a) Federal, State, local, territorial, tribal, foreign-government, and private-sector screening processes, and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.

Id.

twelve preexisting watchlists, including the No Fly List.[193] The FBI, along with other federal agencies, was specifically tasked with coordination of the TSC data collection and the screening processes of multiple streams of data (e.g., immigration and border control data, passport and visa data, and No Fly List and Transportation Security Administration data).[194] The TSC-maintained database combined the No Fly List with other digitally generated watchlists to create one centralized repository for all suspected international and domestic terrorists.[195]

2. No Fly List

Prior to the terrorist attacks of September 11, 2001, the federal government maintained a modest version of the current list known widely as the No Fly List.[196] Previously, the FBI issued directives to air carriers prohibiting the transport of sixteen specific individuals due to the potential terrorist threat they posed to civil aviation.[197] Directly after the terrorist attacks, the FBI launched the "Pentagon/Twin Towers Bombing

193. Mohamed v. Holder, 995 F. Supp. 2d 520, 525 (E.D. Va. 2014) ("In creating the [Terrorist Screening Database], the government consolidated as many as twelve preexisting watchlists, including the No Fly List.").

194. *See* NAT'L COUNTERTERRORISM CTR., WATCHLISTING GUIDANCE, *supra* note 189, at 15.

195. *Id.* at 50 (explaining that the Terrorist Screening Center Policy Board Working Group maintains the criteria and implementation guidance for the No Fly List and Selectee List); *id.* at app. 7, at 2 ("The TSDB consolidates the U.S. Government's terrorism screening and lookout databases into a single integrated identities database. The TSDB is also known as the 'watchlist.'").

196. *See* U.S. DEP'T OF TRANSP., TRANSP. SEC. INTELLIGENCE SERV., POWERPOINT: TSA WATCH LISTS 2 (2002) [hereinafter U.S. DEP'T OF TRANS., TSA WATCH LISTS], *available at* http://www.aclunc.org/cases/landmark_cases/asset_ upload_file371_3549.pdf (released into the public record by the ACLU as part of a settlement agreement in Gordon v. FBI, No. C-03-1779 (N.D. Cal. Jan. 24, 2006)); *see also Mohamed*, 995 F. Supp. 2d at 525. In *Mohamed*, the Court provides the following historical summary of the No Fly List:

> Following the attacks of September 11, 2001, Congress and the President mandated that federal executive departments and agencies share terrorism information with those in the counterterrorism community responsible for national security. Piehota Decl., ¶ 4. Specifically, Congress directed the TSA, "in consultation with other appropriate Federal agencies and air carriers, establish policies and procedures requiring air carriers (A) to use information from government agencies to identify individuals on passenger lists who may be a threat to civil aviation or national security; and (B) if such an individual is identified, notify appropriate law enforcement agencies, prevent the individual from boarding an aircraft, or take other appropriate action with respect to that individual."

Id. (quoting 49 U.S.C. § 114(h)(3) (2012)).

197. *See id.*

Investigation" (PENTTBOM).[198] As an outgrowth of the PENTTBOM investigation and as the FBI developed leads on the potential identity of the 9/11 hijackers, the agency created a separate "Terrorist Watchlist."[199] The FBI subsequently passed the information to the Federal Aviation Administration, which disseminated the information to air carriers.[200]

Soon thereafter, the "no transport list" grew from sixteen names on September 10, 2001, to almost 600 names by December 2001.[201] By that time, the lists of potential terrorists had been reclassified because the government separated transport risks into two lists: a "No Fly List" and a "Selectee List."[202] The No Fly List maintained the names of individuals that air carriers were to deny transport.[203] The "Selectee List" contained names of individuals that air carriers were to select for additional screening prior to boarding an aircraft and additional luggage screening.[204]

C. *Commonality of Big Data Consequences*

Admittedly, each big data blacklisting program discussed in this Article entails distinct administrative and technological structures informed by separate databases, differing algorithms, and different uses of data, including differing data collection and analysis protocols. This Article recognizes that because each program operates within different factual contexts, there is necessarily a differing administrative structure guiding remediation. From a description of the operational impact of nonclassified programs—such as the No Work List, No Vote List, and No Citizenship List—and classified and semi-classified programs—such as the No Fly List and Terrorist Watchlist—the discussion above demonstrates how big data programs operated by the government can assign a heightened suspicion and facilitate inferences of guilt. Heightened suspicion may result from either a data match or a data no-match in a database screening program or digital watchlisting system. Inferences of guilt may appear as labeling an individual as a potential terrorist suspect, a future threat to national security, unlawfully present in the United States, a criminal alien, or as committing identity fraud. As discussed below, data mismatches can trigger heightened suspicion under

198. *9/11 Investigation (PENTTBOM)*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/history/famous-cases/9-11-investigation (last visited Oct. 16, 2015).

199. U.S. DEP'T OF TRANS., TSA WATCH LISTS, *supra* note 196, at 2.

200. *See id.*

201. *Id.* at 3.

202. *Id.*

203. Shane, *supra* note 10, at 812.

204. *Id.*

the database screening protocols in the No Work List (e.g., E-Verify) and the No Vote List (e.g., HAVA).[205] Data matches can also trigger heightened suspicion in database screening protocols in the No Vote List (e.g., SAVE)[206] and the No Citizenship List (e.g., S-COMM/PEP).[207]

III. BIG DATA BLACKLISTING RISKS

Part III explores how big data blacklisting describes those categorized by the government as administratively "guilty until proven innocent" by virtue of suspicious digital data. The big data blacklisting risks described below may appear to be procedural in nature (e.g., failure of notice or failure to offer an appropriate appeals process). However, this Article invites a different perspective—one that views big data harms as imposing administratively a "guilty until proven innocent" status upon entire classes and subclasses of individuals in a way that is inconsistent with fundamental liberty interest protections under substantive due process.

A. *Risks of Nonclassified Big Data Programs*

To help anchor how the government categorizes individuals as "guilty until proven innocent," the discussion below demonstrates how some nonclassified big data programs operated by the government can assign heightened suspicion through data matches or mismatches in the No Work List, No Vote List, and No Citizenship List.

---

205. *See, e.g.*, *Electronic Employment Verification Systems: Needed Safeguards to Protect Privacy and Prevent Misuse: Hearing Before the Subcomm. on Immigration, Citizenship, Refugees, Border Sec., & Int'l Law of the H. Comm. On the Judiciary*, 110th Cong. (2008) ("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 SSN mismatches under HAVA database screening can disenfranchise voters).

206. U.S. DEP'T. OF HOMELAND SEC., U.S. CITIZENSHIP & IMMIGRATION SERVS., *Privacy Impact Assessment for the Systematic Alien Verification for Entitlements Program* (Apr. 19, 2013), http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy-pia-%20uscis-save-20130419.pdf ("If SAVE is unable to find a record pertaining to the applicant or the record has discrepant information or a photo mismatch . . . agencies are required to verbally notify the benefit applicant that they cannot verify the applicant's eligibility [and] that there is an additional manual verification option.").

207. *See, e.g.*, *Secure Communities*, U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, http://www.ice.gov/secure_communities/ (explaining that if ICE detects a match 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.

1. No Work List

E-Verify, unlike the No Fly List, has not faced rigorous due process challenge.[208] Yet, multiple programmatic challenges have plagued E-Verify since its inception, including allegations that it imposes significant barriers to employment opportunities without proper redress opportunities. Many of the difficulties documented by those examining the E-Verify system show why and how big data database screening programs are problematic.[209] A fundamental issue begins with questioning the underlying databases and the reliability of the data that informs the database screening protocol.

In a 1997 report and a 2002 follow-up report, the Inspector General of the DOJ concluded that the underlying data supporting the E-Verify system provided by the Immigration and Naturalization Service (INS), the predecessor of the U.S. Citizenship and Immigration Services (USCIS), was "flawed in content and accuracy."[210] Despite technological attempts to upgrade the system over the past decade, such as requiring employers to double-check the data they have inputted and directly linking the E-Verify system to USCIS databases, multiple challenges remain with the system.[211] A 2007 evaluation of E-Verify conducted by Westat, an independent research organization contracted by DHS, concluded that the accuracy of E-Verify had improved substantially from its initiation but that the error rate was still too high to allow for the mandatory expansion of the pilot program.[212] The report specifically determined that "the database used for verification is still not sufficiently

208. Employers, however, have raised some due process challenges to parts of E-Verify; none have been successful. *See* KEVIN R. JOHNSON ET AL., UNDERSTANDING IMMIGRATION LAW 137–38 (2012).

209. *See, e.g.*, Stumpf, *Getting to Work*, *supra* note 16; 2009 WESTAT REPORT, *infra* note 227.

210. U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., REP. NO. I-2003-001, INSPECTIONS REPORT: IMMIGRATION. AND NATURALIZATION SERVICE'S ABILITY TO PROVIDE TIMELY AND ACCURATE ALIEN INFORMATION TO THE SOCIAL SECURITY ADMINISTRATION 25 (2002), *available at* http://www.justice.gov/oig/reports/INS/e0301/final.pdf. *See generally* U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., REP. NO. I-97-08, IMMIGRATION AND NATURALIZATION SERVICE MONITORING OF NONIMMIGRANT OVERSTAYS (1997), *available at* http://www.justice.gov/oig/reports/INS/e9708/index.htm; U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., FOLLOW-UP REPORT ON INS EFFORTS TO IMPROVE THE CONTROL OF NONIMMIGRANT OVERSTAYS, REP. NO. I-2002-006 (2002), *available at* http://www.justice.gov/oig/reports/INS/e0206/index.htm.

211. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-146, EMPLOYMENT VERIFICATION: FEDERAL AGENCIES HAVE TAKEN STEPS TO IMPROVE E-VERIFY, BUT SIGNIFICANT CHALLENGES REMAIN (2010) [hereinafter GAO, 2010 E-VERIFY REPORT], *available at* http://www.gao.gov/assets/320/314278.pdf.

212. WESTAT, FINDINGS OF THE WEB BASIC PILOT EVALUATION xxi (2007) [hereinafter 2007 WESTAT REPORT], *available at* http://www.uscis.gov/sites/default/files/files/article/WebBasicPilotRprtSept2007.pdf (report submitted to DHS).

up to date to meet the IIRIRA requirement for accurate verification"[213]

Discrepancies in the underlying databases, human error in inputting data and accessing the system, and other administrative and technological complications have resulted from the aggregation and maintenance of the E-Verify database screening system.[214] For example, a 2006 analysis conducted by SSA of its own databases revealed that an estimated 17.8 million records, or 4.1% contained discrepancies related to name, date of birth, or citizenship status and that 12.7 million of these pertained to U.S. citizens.[215] A U.S. Government Accountability Office (GAO) investigation later determined that between one and four percent of lawful immigrants' "A" files (alien number and record), the primary record for all immigrants in the United States, were missing.[216] The rate of error was considerably higher in regions of the nation with the most active filings, such as the San Diego field office, where nearly 21% of all records were missing.[217]

Other records accessed by the E-Verify system are still in analog form. The paper-based files maintained by DHS and other federal agencies are in a conversion process to allow for the development of electronic formats.[218] Yet, the process of converting data from an analog, paper-based form to a digital, machine-searchable form leaves room for additional human error.[219]

Furthermore, misspellings and incorrect name order lead to data mismatches under the E-Verify database screening system despite the fact that SSA algorithms allow for some variation in name order and that there is a manual check that comes with contesting a TNC.[220] This particular problem disproportionately affects women, because of name changes due to marriage or divorce, and minorities because foreign

213. *Id.*

214. DORIS MEISSNER & MARC R. ROSENBLUM, MIGRATION POLICY INST., THE NEXT GENERATION OF E-VERIFY GETTING EMPLOYMENT VERIFICATION RIGHT 6 (2009), *available at* http://www.migrationpolicy.org/pubs/Verification_paper-071709.pdf.

215. SOC. SEC. ADMIN., OFFICE OF INSPECTOR GEN., A-08-06-26100, CONGRESSIONAL RESPONSE REPORT: ACCURACY OF THE SOCIAL SECURITY ADMINISTRATION'S NUMIDENT FILE, ii, 6 (2006), *available at* http://oig.ssa.gov/sites/default/files/audit/full/pdf/A-08-06-26100_0.pdf.

216. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-85, IMMIGRATION BENEFITS: ADDITIONAL EFFORTS NEEDED TO HELP ENSURE ALIEN FILES ARE LOCATED WHEN NEEDED 3–4 (2006), *available at* http://www.gao.gov/assets/260/252947.pdf.

217. *Id.* at 4.

218. *See, e.g.*, *RAPID I-9: Streamlined Electronic I-9 & E-Verify*, A-CHECK (Mar. 2010), http://www.acheckamerica.com/media/1638/2012-004_RAPID_I-9-Electronic_I-9_and_E-Verify.pdf.

219. MEISSNER & ROSENBLUM, *supra* note 214, at 6.

220. Name-order errors were also a problem during the 2004 and 2008 U.S. elections when the government denied many Asian Americans voting rights as a result. *See, e.g.*, ASIAN AM. LEGAL DEF. & EDUC. FUND, ASIAN AMERICAN ACCESS TO DEMOCRACY IN THE 2008 ELECTIONS 4, 9 (2009), *available at* http://aaldef.org/docs/AALDEF_Election_2008_Report.pdf.

names are more often transposed.[221] Moreover, the databases linked to E-Verify must constantly be updated as persons change their names, or as the immigration or citizenship status of an individual is corrected.[222] The E-Verify system has faced challenges in staying current with the adaptations to the government databases as they unfold on a minute-by-minute basis.[223]

Experts have concluded that these factors together create a database screening system that is unreliable and inaccurate in its structure, both technologically and programmatically, as well a system that has led to widespread discriminatory results in its application. In the 2007 Westat report, while E-Verify confirmed U.S. citizens automatically 96% of the time, the rate dropped to 72% for lawful permanent residents and only 63% for other lawful immigrants authorized to work in the United States.[224] Overall, the proportion of inquiries that produce TNCs has decreased to almost 2.6% from the 8% that existed from 2004 to 2007.[225] The percentage of these TNCs that are erroneous, however, "remains alarmingly high."[226] According to one estimate, the government issues 22% of all TNCs to lawful workers,[227] while another study places the number at a shocking 95% erroneous TNC rate.[228] Of the TNCs that the government erroneously issues and that individuals later contest and resolve, error rates are approximately 0.1% for native-born U.S. citizens, 1% for lawful permanent residents, 3.2% for foreign-born citizens, and 5.3% for legal non-immigrants, such as temporary workers and other noncitizens who are authorized to work.[229] This means that the erroneous mismatch rate is thirty times higher for foreign-born workers than for those born in the United States and ninety-eight times higher for naturalized citizens than native-born citizens.[230]

According to various reports, the average time from the date on which a worker originally receives a TNC to the resolution of an E-Verify

221. *See* MEISSNER & ROSENBLUM, *supra* note 214, at 6.

222. *See id.*

223. *Id.*

224. 2007 WESTAT REPORT, *supra* note 212, at 148.

225. GAO, 2010 E-VERIFY REPORT, *supra* note 211, at 16.

226. MARC R. ROSENBLUM, MIGRATION POLICY INST., E-VERIFY: STRENGTHS, WEAKNESSES, AND PROPOSALS FOR REFORM 7 (2011), *available at* http://www.migrationpolicy.org/pubs/E-Verify-Insight.pdf.

227. *Id.* at 7; *see also* WESTAT, FINDINGS OF THE E-VERIFY PROGRAM EVALUATION (2009) [hereinafter 2009 WESTAT REPORT], *available at* www.uscis.gov/USCIS/E-Verify/E-Verify/Final%20E-Verify%20Report%2012-16-09_2.pdf (report submitted to DHS).

228. ROSENBLUM, *supra* note 226, at 7.

229. 2009 WESTAT REPORT, *supra* note 227, at 208–11.

230. *See* 2007 WESTAT REPORT, *supra* note 212, at xxv–vi.

dispute can range from 12.5[231] to 39.7 days.[232] If the matter cannot be resolved, the federal government has the discretion to issue a "Case in Continuance" within the E-Verify system.[233] While the government attempts to resolve the data mismatch with the employee, the employee is often not allowed to work with an intended employer.[234] The fact that many Americans lack the personal documentation necessary to correct an error exacerbates difficulties in resolving data mismatches under the E-Verify system. A 2006 study by the Brennan Center for Justice estimated that 21 million U.S. citizens lack valid identity documents.[235] For example, 13 million U.S. citizens do not have access to passports, birth certificates, or naturalization papers needed to prove citizenship (and, in this case, work authorization).[236]

Studies have indicated that many employees, particularly those who are economically disadvantaged, become discouraged and fail to resolve the mismatch, or employers discourage them from contesting the TNC result in the E-Verify system.[237] Some employers secretly prescreen employees through the E-Verify system and fail to notify an employee that she has a right to resolve the system error.[238] Eighty-five percent of all TNCs are uncontested.[239]

DHS argues that it monitors E-Verify use by "closely monitor[ing] uncontested mismatches and actively reach[ing] out to employers to ensure that they are aware of their responsibility to inform employees of the right to contest."[240] However, Westat and other experts studying the E-Verify system have questioned whether this monitoring of the system is sufficient, particularly given the evidence that suggests that the E-Verify pilot program is subject to employer misuse and abuse. Numerous studies have reported finding that "employers do not always follow Federally mandated safeguards," that "not all employers inform their employees of verification problems," and that lawful workers are

231. 2009 WESTAT REPORT, *supra* note 227, at 91.

232. 2007 WESTAT REPORT, *supra* note 212, at E-4.

233. U.S. CITIZENSHIP & IMMIGRATION SERVS., E-VERIFY QUICK REFERENCE GUIDE FOR EMPLOYERS 16 (2010), *available at* http://www.uscis.gov/sites/default/files/USCIS/E-Verify/Customer%20Support/E-Verify%20Quick%20Reference%20Guide%20for%20Employers%20R3%200-%20Final.pdf.

234. GAO, 2010 E-VERIFY REPORT, *supra* note 211.

235. BRENNAN CTR. FOR JUSTICE, CITIZENS WITHOUT PROOF: A SURVEY OF AMERICANS' POSSESSION OF DOCUMENTARY PROOF OF CITIZENSHIP AND PHOTO IDENTIFICATION 3 (2006), *available at* http://www.brennancenter.org/page/-/d/download_file_39242.pdf.

236. *Id.* at 2.

237. *See id.* at 1, 3.

238. *See* 2007 WESTAT REPORT, *supra* note 212, at 46.

239. *Id.* at 49.

240. U.S. DEP'T OF HOMELAND SEC., U.S. CITIZENSHIP & IMMIGRATION SERVS., E-VERIFY STATISTICS, *available at* http://www.uscis.gov/site-hierarchy/13298/e-verify-program-statistics.

consequently "denied not only jobs, but also the opportunity to resolve any inaccuracies in their Federal records."[241]

A high percentage of employers failed to inform workers that E-Verify produced a TNC in connection with their name. This resulted not only in a deprivation of an opportunity to correct a false mismatch in the E-Verify database system, but also led to the deprivation of an employment opportunity. An early study of the program revealed that 73% of workers whom employers should have notified of a TNC were not notified, resulting in E-Verify producing a FNC.[242] In a more recent study of E-Verify, 98% of employers reported always notifying workers of TNCs, but only 58% of individuals who were the subject of TNCs recalled employers notifying them, and only 28% of their employee files contained signed copies of the notification form.[243] Similarly, while 76% of employers claimed to always explain the meaning of a TNC to individuals receiving them, 54% of workers who had received TNCs did not recall receiving an explanation.[244]

As a result, violations of the E-Verify system functionally become invisible and uncontestable due to the virtual nature of the database screening process. Workers, including U.S. citizens and other lawful immigrants, are unable to challenge erroneous government records or potentially inaccurate data screening protocols due to database prescreening that employers conduct in secret. The programmatic challenges that have accompanied the E-Verify pilot system thus far "illustrate[] the fundamental problem with E-Verify: workers are presumed unauthorized for employment unless they prove otherwise."[245]

DHS has attempted to take corrective action.[246] USCIS launched the Compliance Tracking and Management System in 2009 to monitor the

241. INST. FOR SURVEY RESEARCH, TEMPLE UNIV. & WESTAT, INS BASIC PILOT EVALUATION SUMMARY REPORT 19–20 (2002), *available at* https://web.archive.org/web/20111018173337/http://www.nilc.org/immsemplymnt/ircaempverif/basicpiloteval_westat&temple.pdf [hereinafter BASIC PILOT REPORT].

242. *Id.* at 20.

243. *See* 2009 WESTAT REPORT, *supra* note 227, at 104, 153–56.

244. *Id.* at 153–54.

245. *E-Verify System: DHS Changes Name, but Problems Remain for U.S. Workers*, ELEC. PRIVACY INFO. CTR. (July 2007), http://epic.org/privacy/surveillance/spotlight/0707/.

246. *See, e.g.*, U.S. DEP'T. OF HOMELAND SEC., U.S. CITIZENSHIP AND IMMIGRATION SERVS., E-VERIFY, *Employee Email Notifications*, http://www.uscis.gov/e-verify/employees/employee-email-notifications. DHS has attempted to correct notice deficiencies related to the E-Verify program through the introduction of an email notification program. *Id.* Employers entering personally identifiable data into the E-Verify database screening protocol must include an email address if an employee provides one to the employer:

> This latest enhancement to E-Verify is made possible by the new Employment Eligibility Verification Form I-9. Employees will notice a new optional data field

compliance of employers enrolled in the program.[247] Additionally, on March 21, 2011, USCIS introduced E-Verify Self Check, which allows a prospective employee to go online to correct data errors.[248] If employment authorization cannot be confirmed, individuals receive information on how to resolve potential data mismatches.[249] Because Self Check is untested, its remedial impact on the E-Verify system is unknown. Self Check may in fact open the E-Verify system to other data vulnerabilities and programmatic challenges.

From empirical studies evaluating the efficacy of E-Verify, it appears that employers may have denied up to 189,000 U.S. citizens and other authorized workers employment opportunities under the database screening program.[250] Appendix A provides an example of some of the consequences faced by individuals alleging employment deprivations by the government as a result of the program.

2. No Vote List

To vote, a person's name must appear on the voter registration roll maintained by the county in which he votes.[251] States will occasionally purge names from their voter rolls, ostensibly to ensure that only those eligible to vote can do so.[252] A report from thirty-nine states and the District of Columbia, for example, stated that local governments purged

---

> in Section 1 of the revised Form I-9 asking for the employee's email address; this update allows employees to voluntarily provide their email address. When the employee provides an email address on Form I-9, employers *must* enter it into E-Verify. The new email notification process does not replace the current TNC process. Employers are still required to notify employees of TNCs and their right to contest.

Id.

247. U.S. DEP'T OF HOMELAND SEC., U.S. CITIZENSHIP & IMMIGRATION SERVS., E-VERIFY: HISTORY AND MILESTONES 4 (2014), *available at* http://www.uscis.gov/e-verify/about-program/history-and-milestones.

248. U.S. DEP'T OF HOMELAND SEC., U.S. CITIZENSHIP & IMMIGRATION SERVS., DHS LAUNCHES E-VERIFY SELF CHECK FACT SHEET (2011), *available at* http://www.uscis.gov/news/dhs-launches-e-verify-self-check-fact-sheet.

249. *Id.*

250. GAO, 2010 E-VERIFY REPORT, *supra* note 211, at 16. In fiscal year 2009, "about 189,000 [new hires], received a [Final Nonconfirmation under E-Verify] because their employment eligibility status remained unresolved." *Id.*

251. MYRNA PÉREZ, BRENNAN CTR. FOR JUSTICE, VOTER PURGES 1 (2008), *available at* https://www.brennancenter.org/sites/default/files/legacy/publications/Voter.Purges.f.pdf.

252. *See, e.g.*, Zachary Roth, *Ken Cuccinelli's Voter Purge in Virginia*, MSNBC (Oct. 18, 2013, 2:21 PM), http://www.msnbc.com/msnbc/ken-cuccinellis-voter-purge.

13 million people from voter rolls from 2004 to 2006.[253]

Thus, it is important to look at examples of states that have attempted to purge their voter rolls and examine concrete examples of eligible voters who found themselves removed from a local voter roll due to database error or human error. The HAVA database screening system, relying upon SSA's database, and the SAVE database screening protocol, relying upon the immigration records databases of DHS, have been criticized as being particularly unreliable for voter purges.[254] Appendix B gives details on the challenges and consequences that can accompany voter purges through database screening.

3. No Citizenship List

Since its inception in 2008, as explained above, S-COMM/PEP has facilitated state and local law enforcement data sharing with the FBI and DHS, including data sharing through biometric database screening (e.g., digital fingerprints).[255] S-COMM has been criticized for targeting non-criminal offenders and for other inefficacies.[256] The database, for example, has been criticized as outdated and error-prone and the database screening protocol appears to facilitate the unlawful detention and deportation of U.S. citizens over whom the ICE has no authority.[257]

---

253. PÉREZ, *supra* note 251, at 1 (citing U.S. ELECTION ASSISTANCE COMM'N, THE IMPACT OF THE NATIONAL VOTER REGISTRATION ACT OF 1993 ON THE ADMINISTRATION OF ELECTIONS FOR FEDERAL OFFICE 2005–2006: A REPORT TO THE 110TH CONGRESS 50 (2007), *available at* http://www.eac.gov/assets/1/Page/NVRA%20Reports%20and%20Data%20Sets%202006-2005.pdf).

254. *See, e.g.*, *id.* at 22.

255. U.S. DEP'T OF HOMELAND SEC., IMMIGRATION & CUSTOMS ENFORCEMENT, SECOND CONGRESSIONAL STATUS REPORT COVERING THE FOURTH QUARTER FISCAL YEAR 2008 FOR SECURE COMMUNITIES: A COMPREHENSIVE PLAN TO IDENTIFY AND REMOVE CRIMINAL ALIENS 8–10 (2008) ("The Interoperability pilot, also known as interim Data Service Model (iDSM), was launched in September 2006. . . . [And] "ICE plan[ned] to move Interoperability to full production at the first pilot site in October 2008."), *available at* http://www.ice.gov/doclib/foia/secure_communities/congressionalstatusreportfy084thquarter.pdf.

256. *See, e.g.*, MOTOMURA, *supra* note 20, at 83 (S-COMM "exposes unauthorized migrants with no criminal record or only minor convictions to deportation[,]" and in addition, "undermines the relationship between police and immigrant communities"); Cox & Miles, *Policing Immigration*, *supra* note 20, at 134 (explaining that results from empirical evaluation "reveal a disparate impact, but cannot identify disparate treatment—the intentional singling out of a racial or ethnic group"); Lasch, *supra* note 20, at 225 ("[T]here has been a general failure of Secure Communities to hit its target. . . . some seventy-nine percent of immigrants deported through Secure Communities had either no criminal conviction or only a lower level criminal conviction.") (citations omitted).

257. *See, e.g.*, KOHLI ET AL., *supra* note 169, at 4 ("ICE acknowledges that there might be [Automated Biometric Identification System] matches, or hits, for U.S. citizens for a number of reasons, including that naturalization data has not been updated in its databases." (citing *Secure Communities: IDENT/IAFIS Interoperability Monthly Statistics through April 20, 2011*, at 50, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, retrieved from http://www.ice.gov/doclib/foia/

According to one report, as of April 2011, ICE may have erroneously apprehended approximately 3600 U.S. citizens through the use of the S-COMM biometric database screening protocol.[258] These mistakes may result when faulty information finds its way into the S-COMM database screening protocol, and when the database information comes from many sources.[259]

The U.S. government often denies error in the detention and deportation of U.S. citizens. One study has concluded that ICE has not detained or deported any U.S. citizens.[260] Yet, "[a]ccording to ICE records, [from Fiscal Year 2008 to Fiscal Year 2012, immigration] detainers were issued on a total of 834 individuals who were actually U.S. citizens."[261] Additionally, under S-COMM, through erroneous database screening results, it appears that S-COMM mistakenly targeted up to 5880 U.S. citizens for potential detention and deportation.[262] Although it appears that ICE identified the database screening errors prior to the erroneous detention and deportation of the 5880 U.S. citizens, the fact remains that the S-COMM database screening protocols may have wrongfully targeted thousands of U.S. citizens. This potentially indicates programmatic challenges such as inaccurate algorithms, unreliable data in the underlying databases, inaccurate biometric data captured or entered into the database possibly from human error, other implementation failures, or other technological or program management difficulties.

Given the continued debate on this topic, it is important to look at news accounts of those who ICE has unlawfully detained because of database error. Appendix C contains examples of U.S. citizens who ICE

---

sc-stats/nationwide_interoperability_stats-fy2011-feb28.pdf)); CTR. FOR CONSTITUTIONAL RIGHTS, NAT'L DAY LABORER ORG. NETWORK, & CARDOZO SCHOOL OF LAW IMMIGRATION JUSTICE CLINIC, *Briefing Guide to Secure Communities* 3 (2010), *available at* http://ccrjustice.org/sites/default/files/assets/files/Secure%20Communities%20Fact%20Sheet%20Briefing%20guide%208-2-2010%20Production.pdf.

258. KOHLI ET AL., *supra* note 169, at 4 ("[W]e find that approximately 3,600 US citizens have been apprehended by ICE from the inception of the program through April 2011[,]" extrapolating from 1.6% of cases where U.S. citizens were apprehended by ICE in study of "a random national sample of 375 individuals who were identified as 'IDENT-Matches' by the Secure Communities Program").

259. *See id.* 1–2 (explaining that the S-COMM database screening protocol includes forwarding information to the FBI and DHS, and "DHS checks the fingerprints against the Automated Biometric Identification System, also known as IDENT, a fingerprint repository containing information on over 91 million individuals, including travelers, applicants for immigration benefits, and immigrants who have previously violated immigration laws").

260. *See* W.D. Reasoner & Jessica Vaughan, *Secure Communities by the Numbers*, *Revisited (Part 1 of 3): Analyzing the Analysis*, CTR. FOR IMMIG. STUD. (Dec. 2011), http://cis.org/SC-by-the-numbers-critique-part1.

261. TRAC IMMIGRATION, WHO ARE THE TARGETS OF ICE DETAINERS? (2013), *available at* http://trac.syr.edu/immigration/reports/310/.

262. *See* Julia Preston, *U.S. Identifies 111,000 Immigrants with Criminal Records*, N.Y. TIMES (Nov. 12, 2009), http://www.nytimes.com/2009/11/13/us/13ice.html.

erroneously and unlawfully detained, including U.S. citizens subjected to erroneous deportation.

B. *Risks of Classified and Semi-Classified Big Data Programs*

At the dawn of the big data revolution, as explained above, unprecedented governmental access to public and private data led to an unprecedented asymmetric power between the state and citizen. As can be better understood through a careful examination of big data programs that may be informed by classified and semi-classified information gathering systems, the power asymmetries are especially pronounced when national security objectives heighten governmental power while the administrative state objectives may weaken the position of the citizen in relationship to the government.

Big data technologies facilitate the government's ability to search for suspicious data. Therefore, newly emerging big data programs allow for the tracking and isolation of digitally generated data deemed "suspicious," including "suspicious" metadata, "suspicious" associational and geolocational data, "suspicious" correlative data and data patterns, and other mass integrative record data and algorithmic matching data that can be construed as "suspicious." One of the key risks, therefore, is an inability to remediate one's "guilty until proven innocent" status. Overcoming the inferential guilt facilitated by big data tools may be nearly impossible due to the classified and semi-classified position of the data that has singled out individuals for suspicion. Algorithmic intelligence systems structured to support big data programs, and defended as statistically accurate, may be nearly impossible to challenge as well.

1. Terrorist Watchlist

Due to the classified nature of the intelligence that informs the fulfillment of the unclassified criteria for placement on a terrorist watchlist, an individual's ability to understand and challenge their inclusion on a watchlist is limited.[263] "The lesser standard for inclusion in the broader TSDB . . . requires a reasonable suspicion that the individual is a known or suspected terrorist."[264] The criteria for inclusion

263. *See, e.g.*, Defendants' Consolidated Memorandum in Support of Cross-Motion for Partial Summary Judgment and Opposition at 52, Latif v. Holder, No. 3:10-CV-00750-BR (D. Or. May 28, 2015) (stating that when faced with the reasons for a nomination to the No Fly List, the United States has argued "such inquiries would inevitably seek to scrutinize reasons for the No Fly determination and support for them—the vast majority of which would implicate classified national security and law enforcement information").

264. *Id.* at 5 n.3 (citing Declaration of TSC Deputy Director for Operations G. Clayton Grigg,

on the No Fly List require a higher standard. Specifically, the United States has explained that "any individual, regardless of citizenship, may be placed on the No Fly List if the TSC determines that he or she represents: a threat of committing an act of international terrorism . . . or an act of domestic terrorism."[265]

According to a public report issued by the DOJ's Office of the Inspector General, names "enter the master TSDB through a so-called 'nomination process.'"[266] Staff from the FBI and TSC assess levels of terrorist-related suspicion based upon "'whether or not the person is an appropriate candidate for inclusion' on the consolidated watch list and 'whether or not sufficient identifying information is available.'"[267] The nomination and determination process has been criticized for its failure to rigorously and individually assess appropriate inclusion. It has also been criticized for a lack of any minimum qualitative guideline or quantitative baseline for investigatory or evidentiary standards.[268]

"[T]he U.S. Government's consolidated Terrorist Screening Database (TSDB) [is] often referred to as the 'Terrorist Watchlist,' and serves as a bridge between law enforcement, Homeland Security, the Intelligence

---

May 28, 2015 (Grigg Decl.) ¶ 15).

265. *Id.* (citing See Gen. Stipulations [Dkt. No. 173] ¶ 5; Declaration of TSC Deputy Director for Operations G. Clayton Grigg, May 28, 2015 (Grigg Decl.) ¶ 17.3). The specific criteria for inclusion on the No Fly List includes:

> [1] a threat of committing an act of international terrorism (as defined in 18 U.S.C. § 2331(1))[;]
>
> [2] or [a threat of committing] an act of domestic terrorism (as defined in 18 U.S.C. § 2331(5)) with respect to an aircraft (including a threat of air piracy, or threat to an airline, passenger, or civil aviation security);
>
> [3] or a threat of committing an act of domestic terrorism (as defined in 18 U.S.C. § 2331(5)) with respect to the homeland;
>
> [4] or a threat of committing an act of international terrorism (as defined in 18 U.S.C. § 2331(1)) against any U.S. Government facility abroad and associated or supporting personnel, including U.S. embassies, consulates and missions, military installations (as defined by 10 U.S.C. § 2801(c)(4)), U.S. ships, U.S. aircraft, or other auxiliary craft owned or leased by the U.S. Government;
>
> [5] or a threat of engaging in or conducting a violent act of terrorism and who is operationally capable of doing so.

Id.

266. Shane, *supra* note 10, at 815–16 (citing AUDIT DIV., OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, Audit Rep. 05-27, Review of the Terrorist Screening Center 41–43 (2005) (redacted for public release), *available at* http://www.usdoj.gov/oig/reports/FBI/a0527/final.pdf).

267. *Id*. at 816 (citation omitted).

268. *See, e.g.*, *id*. at 816–17.

Community, and international partners."[269] Because the TSC databases and Terrorist Watchlist contain classified information, it is difficult to confirm or interrogate the protocols, methodologies, and other systems in which the government compiles, maintains, analyzes, and utilizes the digital watchlists for policy making.

2. No Fly List

Currently, the FBI, through the TSC, develops and maintains the No Fly List, which consists of the names of individuals whom airlines serving or flying within the United States may not transport.[270] The No Fly List is a subset of the TSDB, and DHS defines it as "a list of individuals who are prohibited from boarding an aircraft."[271] In other words, the government prohibits most individuals on the list from flying into, out of, or over Canadian and American airspace.[272] The Selectee List, another subset of the TSDB, is "a list of individuals who must undergo additional security screening before being permitted to board an aircraft."[273]

In recent years, litigation has forced the disclosure of information on what specific data ultimately supports a decision to place an individual on the No Fly List. Scholars have noted concerns associated with a combination of public–private intelligence-gathering partnerships that focus on data capture and data analytics.[274] In particular, criticism has been leveled that these public–private data partnerships "have enabled the Executive to operate outside of the congressionally imposed framework of court orders and subpoenas, and also outside of the ambit of inter-branch oversight."[275] Regarding due process safeguards and other constitutional concerns, some suggest that the private data gathering conducted by TSC potentially surpasses *ex ante* constitutional protections, while also removing any remaining ex post facto protections.[276]

---

269. *About the Terrorist Screening Center*, FED. BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, *available at* https://www.fbi.gov/about-us/nsb/tsc/about-the-terrorist-screening-center.

270. Tarhuni v. Holder, 8 F. Supp. 3d 1253, 1262 (D. Or. 2014).

271. Mohamed, *supra* note 193 (quoting the declaration of Christopher M. Piehota, appointed director of the Terrorist Screening Center (TSC) on April 10, 2013) (Piehota Decl., ¶ 16).

272. *Id*.

273. *Id*. (Piehota Decl., ¶ 16).

274. *See generally* O'HARROW, *supra* note 31; PRIEST & ARKIN, *supra* note 31; Jon D. Michaels, *All the President's Spies: Private–Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901 (2008).

275. *See id*. at 904.

276. *See id.* (stating that these agreements "leave Congress and the courts ill-equipped . . . to intervene to remedy individual instances or patterns of injustice").

Although TSC is the final arbiter on whether an individual remains in the TSC database, TSC does not accept redress inquiries.[277] Rather, an individual petitioning to have their name removed from either the No Fly List or Selectee List must submit a form to DHS Traveler Inquiry Redress Program (DHS TRIP).[278] DHS TRIP then communicates the inquiry to TSC, which makes a decision on the redress request without providing any further information.[279] TSC notifies DHS TRIP of the decision, and DHS TRIP, in turn, contacts the petitioner.[280] Until recently, despite a decision on the status of the No Fly List petitioner, DHS TRIP's final communication with the petitioner "neither confirms nor denies the existence of any terrorist watch list records relating to the individual" and further does not state whether the individual may fly in the future.[281] In effect, individuals previously had no way to confirm their placement on the No Fly List unless they were denied entry onto a commercial airplane.

The No Fly List litigation forced a revision of the prior notice and redress procedures after it was found to be procedurally defective under procedural due process.[282] These revised redress procedures for the No

277. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-06-1031, TERRORIST WATCH LIST SCREENING: EFFORTS TO HELP REDUCE ADVERSE EFFECTS ON THE PUBLIC 31 (2006) [hereinafter GAO, TERRORIST WATCH LIST SCREENING], *available* at http://www.gao.gov/assets/260/251875.pdf; *see also TSC Redress Procedures*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/nsb/tsc/tsc_redress (last visited Oct. 16, 2015).

278. *See* 49 U.S.C. § 44903(j)(2)(G)(i) (2012) (requiring the TSA to "establish a timely and fair process for individuals identified as a threat under [the screening system] to appeal to the [TSA] the determination and correct any erroneous information"); *id.* § 44926(a) ("The Secretary of Homeland Security shall establish a timely and fair process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat under the regimes utilized by the [TSA].").

279. *See* LIZZY GARY, PRIVACY IMPACT ASSESSMENT UPDATE FOR THE DHS TRAVELER REDRESS INQUIRY PROGRAM (DHS TRIP) 2 (2013), *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pia-update-dhs-all-dhstrip-20130605.pdf.

280. *Id.* at 4.

281. GAO, TERRORIST WATCH LIST SCREENING, *supra* note 277, at 31. For example, the letter addressed to one of the plaintiffs in *Latif v. Holder* stated:

> Security procedures and legal concerns mandate that we can neither confirm nor deny any information about you which may be within federal watchlists or reveal any law enforcement sensitive information. However, we have made any corrections to records that our inquiries determined were necessary, including, as appropriate, notations that may assist in avoiding instances of misidentification.

Memorandum of Points and Authorities in Support of Plaintiff's Opposition to Defendant's Motion to Dismiss at 3 n.1, Latif v. Holder, No. 10-CV-750-BR, 2011 WL 1667471 (D. Or. May 3, 2011) (internal quotation marks omitted).

282. *See* Defendants' Consolidated Memorandum in Support of Cross-Motion for Partial Summary Judgment and Opposition at 273, Latif v. Holder,No. 3:10-cv-00750-BR (D. Or. May 28, 2015).

Fly List became available to the public in March 2015.[283]

Under the new redress procedures, individuals trying to challenge their inclusion on the No Fly List may receive "notice" of their inclusion.[284] The redress procedures, thus, may not provide individuals with any summary of information at all in some circumstances.[285] Further, "[b]ecause No Fly List determinations are typically based on sensitive and classified information, this summary necessarily may not reflect the complete factual basis for inclusion."[286] The redress procedures, thus, may provide individuals with an incomplete summary of information in other circumstances.[287] The new redress procedures do not include procedurally guaranteed access to the underlying evidence that may have led to one's nomination to the No Fly List (e.g., collected data, witness statements, and reports).[288] The new redress procedures further do not include live adversarial proceedings that provide a challenger an opportunity to confront witnesses, interrogate the scientific validity of the methods that led to deprivation, or analyze or dispute the evidence compiled against the individual.[289]

The revised redress procedures do not appear to provide a method to determine whether an individual is on the Selectee List.[290] However, the possibility of an internal administrative appeal or judicial review in a U.S. Court of Appeals exists under 49 U.S.C. § 46110.[291] Travelers may also attempt to preemptively determine their status by opting in to the TSA's Pre-Check system,[292] which expedites screening (and ostensibly

283. *Id.*

284. *Id.* (citing Notice Regarding Revisions to DHS TRIP Procedures [Dkt. No. 197]; Declaration of Deborah O. Moore, Branch Manager of the Transportation Security Redress Branch in the Office of Civil Rights & Civil Liberties, Ombudsman and Traveler Engagement at TSA, May 28, 2015 (Moore Decl.) ¶¶ 12–13).

285. *Id.*

286. *Id.* at 34 (citing Dkt. No. 173 ¶¶ 17–18; Grigg Decl. ¶ 46; Moore Decl. ¶¶ 18–19).

287. *Id.*

288. *Id.* at 39 (stating that according to the United States, "Plaintiffs should not be granted the right to crossexamine individuals, let alone any sources of intelligence or investigative information provided to the Government, in this national security context").

289. *Id.* at 40 (stating that according to the United States, "the specific circumstances strongly weigh against a live adversarial hearing to contest No Fly determinations").

290. DHS explains that "[t]he U.S. government does not reveal whether a particular person is on or not on a watchlist." U.S. DEP'T OF HOMELAND SEC., TRANSP. SEC., TRAVELER REDRESS INQUIRY PROGRAM, *Step 1: Should I Use DHS TRIP?*, http://www.dhs.gov/step-1-should-i-use-dhs-trip.

291. Latif v. Holder, 686 F.3d 1122, 1126 (9th Cir. 2012).

292. *See TSA Pre Check*, TRANSP. SEC. ADMIN., http://www.tsa.gov/tsa-pre-check (last visited Oct. 16, 2015).

boarding) by pre-checking credentials against the terrorist database.[293] The DHS Privacy Office noted in a 2006 report that the existing redress procedures and mechanisms varied in both procedure and effectiveness across the many agencies involved in the watchlists and recommended a robust centralized screening procedure.[294] From the published redress procedures, DHS appears to focus redress relating to persons misidentified as being included on a watchlist.[295]

A 2007 DOJ report estimated that the No Fly List contained over 700,000 names and further reported that the list was "increas[ing] by an average of more than 20,000 records each month."[296] A 2012 GAO report noted an increase in individuals denied boarding or selected for screening, but it did not report any data on the specific volume of the current list.[297] At the time, the FBI reported approximately 550,000 names on the No Fly List, including 500 U.S. citizens.[298]

The TSC offers an internal auditing process that periodically determines the appropriateness of an individual's inclusion on the list. For instance, the government removed almost 3700 names between July and October of 2004.[299] However, despite the remedial procedure and internal auditing process, the list has continued to misidentify individuals and produce both false positives and false negatives. For example, individuals denied access to a commercial flight or repeatedly detained include a U.S. Marine returning from Iraq,[300] a U.S. Senator,[301] and a U.S. House Representative.[302] A 2004 audit of the TSC by the DOJ found multiple deficiencies in the watchlist databases—errors of both

293. It remains an open question whether a "pre-checked" passenger could still run afoul of a watchlist by virtue of a database error.

294. MAUREEN COONEY, DEP'T OF HOMELAND SEC., PRIVACY OFFICE, REPORT ON EFFECTS ON PRIVACY AND CIVIL LIBERTIES 16–21 (2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_nofly.pdf.

295. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., TRANSP. SEC., TRAVELER REDRESS INQUIRY PROGRAM, *supra* note 290 ("[I]f you have been selected for secondary screening on multiple occasions you might be able to use DHS TRIP to resolve issues such as misidentification.").

296. *Justice Department Report Tells of Flaws in Terrorist Watch List*, CNN (Sept. 6, 2007), http://www.cnn.com/2007/US/09/06/terror.watchlist/.

297. *See* Andrea Stone, *No-Fly List Maintained by FBI Includes Double the U.S. Citizens Since 2009*, HUFFINGTON POST (June 1, 2012, 3:29 PM), http://www.huffingtonpost.com/2012/06/01/no-fly-list_n_1563261.html.

298. *Id*.

299. Shane, *supra* note 10, at 817.

300. *'No-Fly' List Delays Marine's Iraq Homecoming*, NBC NEWS (Apr. 12, 2006, 11:06 AM), http://www.nbcnews.com/id/12284855/#.UW4K_JO86So.

301. Sara Kehaulani Goo, *Sen. Kennedy Flagged by No-Fly List*, WASH. POST (Aug. 20, 2004), http://www.washingtonpost.com/wp-dyn/articles/A17073-2004Aug19.html.

302. Ted Barrett, *Kennedy Has Company on Airline Watch List*, CNN (Aug. 20, 2004, 7:18 PM), http://www.cnn.com/2004/ALLPOLITICS/08/20/lewis.watchlist/index.html.

overinclusion and underinclusion.[303] Moreover, a later study showed that the list contained unreliable data, with 35% of the names on the list characterized as "outdated."[304]

The potential unreliability of these systems has led critics to question the accuracy of the data-driven programs that have placed an estimated 500 U.S. citizens on the No Fly List,[305] 5000 U.S. citizens on the Terrorist Watchlist,[306] and 15,800 U.S. citizens on the Terrorist Identities Datamart Environment (TIDE) database[307]—the "central repository"[308] of known or suspected international terrorists.[309]

Appendix D summarizes the circumstances of some of the U.S. citizens and lawful permanent residents claiming due process harms resulting from allegedly erroneous placement on the No Fly List.

IV. BIG DATA BLACKLISTING AND THE DUE PROCESS INQUIRY

As explained above, procedural due process is simply the concept enshrined in the Constitution that when the government deprives a citizen of an interest in life, liberty, or property, the citizen is given notice and

303. *See* U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., REVIEW OF THE TERRORIST SCREENING CENTER xiv–xv, 48–66 (2005), *available at* http://www.justice.gov/oig/reports/FBI/a0527/final.pdf (noting incorrect information in records that would tend to produce false positives, but also errors resulting in false negatives).

304. *See Watch Lists*, ACLU, http://www.aclu.org/technology-and-liberty/watch-lists (last visited Oct. 16, 2015).

305. *See, e.g.*, *No-Fly List Doubles in a Year—Now 21,000 Names*, CBS NEWS (Feb. 2, 2012, 3:01 PM), http://www.cbsnews.com/news/no-fly-list-doubles-in-a-year-now-21000-names/; *see also* ACLU Factsheet, *available at* https://www.aclu.org/national-security/factsheet-aclus-challenge-us-governments-no-fly-list.

306. Jeremy Scahill & Ryan Devereaux, *Barack Obama's Secret Terrorist-Tracking System, By the Numbers*, INTERCEPT (Aug. 5, 2014), *available at* https://firstlook.org/theintercept/2014/08/05/watch-commander/; *see also Terrorist Watchlist*, INFO. SHARING ENV'T, http://www.ise.gov/terrorist-watchlist ("The Terrorist Screening Center (TSC) maintains the U.S. government's consolidated Terrorist Watchlist[-]which supports the ability of front line screening agencies to positively identify known or suspected terrorists trying to obtain visas, enter the country, board aircraft, or engage in other activity.").

307. *Terrorist Watchlist*, *supra* note 306 ("The National Counterterrorism Center manages the Terrorist Identities Datamart Environment (TIDE), which serves as the U.S. government's central repository of information on international terrorist identities as established by the Intelligence Reform and Terrorism Prevention Act of 2004. TIDE supports the [U.S. Government's] various terrorist screening systems or 'watchlists' . . . .").

308. *Id.*; *see also* INFO. SHARING ENV'T, ANNUAL REPORT TO THE CONGRESS (2014), *available at* https://www.ise.gov/sites/default/files/2014_ISE_Annual_Report_to_Congress_0.pdf.

309. The total number of individuals in TIDE is estimated to be over 740,000 persons, of which only a small percentage are U.S. citizens. *See, e.g.*, WILLIAM J. KROUSE, CONG. RESEARCH SERV., R42336, TERRORIST WATCH LIST SCREENING AND BRADY BACKGROUND CHECKS FOR FIREARMS 10 (2012), *available at* http://www.fas.org/sgp/crs/terror/R42336.pdf (reporting that as of December 2011, "TIDE contained over 740,000 persons").

an opportunity to be heard.[310] Substantive due process turns on abstract liberty concepts, including "individual dignity and autonomy," "personal identity," and other rights that courts may construe as inalienable.[311] Substantive due process rights are often viewed as a protection of rights that are "deeply rooted in this Nation's history and tradition."[312] Rights that are not "fundamental" or "deeply rooted" are subject to lesser scrutiny. "All other liberty interests may be abridged or abrogated pursuant to a validly enacted state law if that law is rationally related to a legitimate state interest."[313]

Its origins "lie in natural law concepts that predate the doctrine's association with due process," and it holds "that once particular rights became vested in individuals, the legislature [is] without power to rescind those rights."[314] For example, in a recent decision, the Supreme Court held that, under substantive due process, "same-sex couples may exercise the right to marry."[315] In *Obergefell v. Hodges*, the Court explained that "the fundamental liberties protected by this [Due Process] Clause include most of the rights enumerated in the Bill of Rights,"[316] and, further, that historical "principles and traditions . . . demonstrate that the reasons marriage is fundamental under the Constitution apply with equal force to same-sex couples."[317] The Court elaborated that "these liberties extend to certain personal choices central to individual dignity and autonomy, including intimate choices that define personal identity and beliefs."[318] As Richard Fallon observes, substantive due process consists of "what

310. *See* Mathews v. Eldridge, 424 U.S. 319, 332–35 (1976).

311. *See supra* note 70 (citing Obergefell v. Hodges, 135 S. Ct. 2584, 2597 (2015) ("In addition these liberties extend to certain personal choices central to individual dignity and autonomy, including intimate choices that define personal identity and beliefs.") (citing Eisenstadt v. Baird, 405 U.S. 438, 453 (1972); Griswold v. Connecticut, 381 U.S. 479, 484–86 (1965)); Lawrence v. Texas, 539 U.S. 558, 574 (2003) (citation omitted); Washington v. Glucksberg, 521 U.S. 702, 726 (1997) (citation omitted); Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 851 (1992) ("These matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment.").

312. *Glucksberg*, 521 at 721 (citation omitted).

313. *Lawrence*, 539 U.S. at 593.

314. Ryan C. Williams, *The One and Only Substantive Due Process Clause*, 120 YALE L.J. 408, 423 (2010) (citations omitted); *see also* Katharine T. Bartlett, *Tradition as Past and Present in Substantive Due Process Analysis*, 62 DUKE L.J. 535, 540 (2012); Victoria F. Nourse, *A Tale of Two* Lochners*: The Untold History of Substantive Due Process and the Idea of Fundamental Rights*, 97 CALIF. L. REV. 751 (2009).

315. Obergefell v. Hodges, 135 S. Ct. 2584, 2599, 2604–05 (2015).

316. *Id.* at 2597 (citing Duncan v. Louisiana, 391 U. S. 145, 147–49 (1968)).

317. *Id.* at 2599.

318. *Id*. at 2597 (citing Eisenstadt v. Baird, 405 U.S. 438, 453 (1972); Griswold v. Connecticut, 381 U. S. 479, 484–86 (1965)).

the Supreme Court takes to be widely shared intuitions or principles that impose duties on government and define standards of reasonableness that constrain governmental pursuit even of acceptable goals."[319]

A. *Substantive Due Process and Informational Privacy Rights*

The applicability of substantive due process protections as a vehicle to shield individuals from overreaching and normalized government dataveillance under newly emerging big data tools remains a complicated and perhaps wishful potentiality, but one that must be considered. Recent cases like *United States v. Jones*[320] have raised—but largely avoided answering—the question of whether and how the Fourth Amendment might protect individuals from government surveillance in the context of law enforcement investigation.[321] Yet, even if the Fourth Amendment may eventually be found to have teeth enough to post limits on the cybersurveillance of law enforcement authorities, it will provide no assistance to individuals outside the law enforcement context. In the National Surveillance State, big data cybersurveillance and big data bureaucratized surveillance systems often operate administratively across a much broader spectrum than that of law enforcement.[322]

Resorting to the Fifth and Fourteenth Amendments in the form of substantive due process protection of individual privacy in a big data world remains a speculative but perhaps necessary venture if constitutional protections are to keep pace with technological leaps and bounds in the realms of big data cybersurveillance and mass dataveillance. An informational right of privacy is not exactly unprecedented, although it is unestablished and stridently opposed by at least two of the Court's current Justices. In 2011, in concurring opinions in *NASA v. Nelson*,[323] Justices Antonin Scalia and Clarence Thomas criticized the notion that the Constitution might protect informational

319. Fallon, *supra* note 67, at 323.

320. 132 S. Ct. 945 (2012).

321. In *United States v. Jones*, 132 S. Ct. 945 (2012), the majority focused on the government's physical trespass affecting property to find that a violation of the Fourth Amendment had occurred. Two concurring opinions emphasized that the Court's current Fourth Amendment tests (one test relies on trespass, the other is the *Katz* reasonable expectation of privacy test) will be increasingly inapplicable to technology-based cases in the future.

322. The converse is equally true: Where the Fourth Amendment does apply, a party generally will not have to resort to the due process clause. "Where a particular Amendment 'provides an explicit textual source of constitutional protection' against a particular sort of government behavior, 'that Amendment, not the more generalized notion of 'substantive due process' must be the guide for analyzing these claims." Albright v. Oliver, 510 U.S. 266, 273 (1994) (quoting Graham v. Conner, 490 U.S. 386 (1989)).

323. NASA v. Nelson, 562 U.S. 134 (2011).

privacy.[324] Their position is consistent with their broader opposition to the notion of substantive due process in the first place—something that, of course, would vitiate substantive due process as a restraint on big data blacklisting harms.[325]

Nevertheless, the Court in *Nelson* avoided deciding whether a constitutional right of informational privacy exists. Instead, assuming that such a right does exist, it held that it was not offended by the government inquiring into the past history of drug use of private government contractors and employees.[326] Justice Samuel Alito authored the majority opinion, adopting a restrained approach and potentially reflecting the Court's reluctance to recognize or expand a constitutional right to informational privacy. One could speculate that discarding a right to informational privacy at the dawn of big data—when the implications of big data are not fully understood by anyone, let alone the judiciary—may not have seemed prudent to the Court. In fact, cases like *Jones* suggest strongly that the Court may be open to retooling Fourth Amendment doctrine if its current jurisprudence remains incapable of applying effective restraints on cybersurveillance and dataveillance by the government. While *Nelson* is certainly not a bellwether of a similar inclination in the context of due process rights, its restraint may indicate something more than a necessary compromise between Justices of differing ideological outlooks.[327]

---

324. Justice Scalia noted in his concurrence in *Nelson*: "Our due process precedents, even our 'substantive due process' precedents, do not support *any* right to informational privacy." *Id.* at 161 (Scalia, J., concurring); *see also* E. THOMAS SULLIVAN & TONI M. MASSARO, THE ARC OF DUE PROCESS IN AMERICAN CONSTITUTIONAL LAW 152–54 (2013) (explaining that, under the category of an informational right to privacy, "the Court has 'referred broadly to a constitutional privacy 'interest in avoiding disclosure of personal matters'") (citing *Nelson*); s*ee also* Lior Stahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007, 2011 (2010) (arguing that "the constitutional right to information privacy . . . ought to much more closely resemble privacy tort law" and in "constitutional adjudication" the courts should ask three questions: "Whether the information is private," "What the applicable social norms are," and "What social interests are vindicated by privacy"); Lior Stahilevitz, *The Centenarian Who Wasn't, NASA v. Nelson and the Constitutional Right to Information Privacy*, U. CHI. L. SCH. FAC. BLOG (Sept. 23, 2010, 10:37 AM), http://uchicagolaw.typepad.com/faculty/2010/09/the-centenarian-who-wasn't-nasa-v-nelson-and-the-constitutional-right-to-information-privacy.html) (discussing the Court's treatment of the constitutional right to privacy in *Nelson*, concluding that the "applicable frameworks for deciding whether the government's conduct violates the constitutional right to information privacy are by no means sensible").

325. "[T]he very idea of substantive due process has been contested." ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES & POLICIES 571 (5th ed. 2015).

326. "We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*. We hold, however, that the challenged portions of the Government's background check do not violate this right in the present case." Nelson, 562 U.S. at 138.

327. Sullivan and Massaro point out that while conservatives may oppose substantive due

What *Nelson* did was enable precedent on informational privacy rights to survive—precedent that Justices Scalia and Thomas thought should be overruled. The Court identified two cases that have opened the door to the notion of constitutional protection of informational privacy. One was *Whalen v. Roe*,[328] a 1977 case that dealt with an early form of big data—a database storing the identities of persons receiving prescriptions for drugs that New York authorities deemed to be dangerous.[329] *Nelson* also preserved as precedent *Nixon v. Administrator of General Services*.[330] That case concerned a statute[331] that Congress passed in the wake of Watergate and Nixon's resignation that was designed to protect Nixon's presidential records and tapes.[332] Besides the government's interest in collecting the information, the *Whalen* and *Nixon* Courts appeared to be swayed by the fact that the harvest of informational data was the least intrusive means for the government to pursue its legitimate and compelling aims. Litigants in the modern context will need to raise the same query. A case challenging the governmental storage and big data or metadata screening of personally identifiable information will be all the stronger if a litigant can suggest an alternative, more restrictive way to achieve the government end without so broadly violating the privacy of the citizenry.

Both *Whalen* and *Nixon* make clear that raising a substantive due process claim in the modern context would thus prompt a twofold inquiry of big data. First, to determine if the government's accumulation and use of big data poses a constitutional threat, the Court would have to inquire into whether there are safeguards to prevent unauthorized informational access that would violate constitutional informational privacy interests or other means of unwarranted disclosure. Secondly, the Court would need to determine whether the statutory and regulatory framework governing informational privacy has sufficiently kept pace with the technological innovations enabling the government to collect and use big data.

A strong contention is that a government-led big data program, in and of itself, constitutes a substantive due process problem when it results in a "suspicion upon a suspicion" problem (e.g., "suspicion"—digitally-

process rights, there is also strong element of conservatism that joins with liberalism in a suspicion of unrestrained governmental powers. "Conservative libertarians, as well as many liberal progressives, likely regard informational privacy as worthy of constitutional, not merely statutory, protection and thus may favor a more elastic view of due process than a narrow 'history and tradition'-based approach might allow." SULLIVAN & MASSARO, *supra* note 324, at 153.

328. 429 U.S. 589 (1977).

329. *Id.* at 592–93.

330. Nixon v. Adm'r of Gen. Servs., 433 U.S. 425 (1977).

331. Presidential Recordings and Material Preservation Act, Pub. L. No. 93-526, 88 Stat. 1695 (1974).

332. Nixon, 433 U.S. at 431–32.

generated or big data-generated suspicion that the government or its delegates may believe is actionable—based "upon a suspicion"—suspicious digital data or database screening result). Any resort to big data cybersurveillance or mass dataveillance systems, in the context of government programs which grant or deny eligibility for rights or privileges, or programs which may mediate or interfere with freedoms or liberty interests, may pose a constitutional challenge. On this score, those programs that subject individuals to big data blacklisting harms would be subject to strict scrutiny analysis: The government must show that its reliance on big data is necessary and narrowly tailored to the use it is serving, and serves a compelling state interest.[333] Or, in the alternative, in the case of the No Fly List, for instance, the government could be compelled to develop an alternative process: A nomination and appeals system must involve small data processes and human intelligence that an individual can fairly contest (e.g., interrogate witnesses, directly challenge the evidence).

B. *Substantive Due Process Approach to Systemic Big Data Blacklisting Harms*

The Court in *Whalen* initiated a theory of informational privacy rights and the question of whether substantive due process should encompass privacy expectations related to the collection and use of digital data, including database systems. A procedural due process approach may appear to be the most logical given the framework that courts use to analyze both substantive and procedural due process deprivations. This Article, however, contends that digital watchlisting and database screening systems should be critiqued collectively; thus, the focus of the constitutional inquiry should be on the protections afforded by substantive due process. Unlike many other constitutional claims that are fact-dependent and generally center around individual rights, due process doctrine generally, and substantive due process in particular, can be viewed as a systemic-type remedy to address system-wide harms.[334] Additionally, procedural due process assumes that mediation of a right was itself proper, whereas substantive due process interrogates the propriety of the mediation of a fundamental right in the first instance.[335]

---

333. *See, e.g.*, Daskal, *supra* note 33, at 377 ("A searching inquiry into the No Fly List, for example, reveals the way it burdens, albeit without extinguishing, long-recognized interests in interstate travel, association, and pursuit of employment of one's choosing. . . . Ultimately, the courts should be pushing the Executive toward a narrow tailoring of restraint to need.").

334. *See, e.g.*, Fallon, *supra* note 67, at 311 ("[A]lthough we characteristically think of constitutional rights in individualistic terms, due process doctrine has developed a strikingly managerial aspect.").

335. *See, e.g.*, Nathan S. Chapman & Michael W. McConnell, *Due Process as Separation of*

Consequently, under procedural due process, the court focuses its inquiry on the method of mediation (e.g., evidentiary hearing, notice, and an impartial judge),[336] whereas under substantive due process, the court typically engages a strict scrutiny review to analyze the precise issue before it (e.g., whether a compelling state purpose supports the government action).[337]

Therefore, this Article seeks to explore a more holistic approach, one that moves beyond critiquing discrete big data programs and instead stresses the commonalities between these various government programs. Looking at the harms of these programs collectively may provide the theoretical vista for conceptualizing how big data blacklisting is, in itself, a substantive due process violation. This is a complex undertaking, and future scholarship on this subject will explore the analytical framework of substantive due process in the context of the mass harms of big data blacklisting. But for the present, this Article is necessarily more descriptive—delineating the general contours of big data blacklisting as a technique of governance and suggesting that procedural due process may be inadequate to remedy big data blacklisting harms.

CONCLUSION

This Article asks whether procedural and substantive due process protections, as currently constructed, fail to address big data blacklisting harms. Big data blacklisting impacts fundamental constitutional rights when digital data is flagged as "suspicious" through big data tools and data tracking systems, and when individuals are categorized as "guilty until proven innocent" through big data-generated inferential guilt. It contends that big data blacklisting harms are not just procedural in nature—that the government has failed to offer proper procedures for remediation of these harms—but that big data dataveillance systems may obstruct fundamental liberty interests. It poses the following question: whether freedom from big data blacklisting harms should be protected as a cognizable fundamental liberty interest under substantive due process.

In seeking to critique the constitutional impact of multiple big data programs collectively, this Article attempts to identify a constitutionally

---

Powers, YALE L.J. 1672, 1679 (2012) ("The distinctive aspect of modern 'substantive due process' . . . is its treatment of natural liberty as inviolate, even as against prospective and general laws passed by the legislature and enforced by means of impeccable procedures.").

336. *See, e.g.*, Cole, *supra* note 1, at 508 ("If the state seeks to take an individual's liberty or property, it must generally ensure that he has notice of the basis for its action and a meaningful opportunity to defend himself.").

337. Fallon, *supra* note 67, at 314 ("[G]overnment intrusions on so-called 'fundamental' rights are subject to 'strict' or exacting scrutiny, a test sometimes formulated as inquiring whether a burden is necessary to promote a 'compelling state interest.'" (citing, *e.g.*, Foucha v. Louisiana, 112 S. Ct. 1780, 1804 (1992) (Thomas, J., dissenting); Carey v. Population Servs. Int'l, 431 U.S. 678, 684–91 (1977); Roe v. Wade, 410 U.S. 113, 155 (1973))).

cognizable harm across the multiple big data blacklisting programs discussed. Additionally, because the traditional legal framework guiding due process analysis is often equipped to handle discrete harms that stem from individualized government programs and specific administrative procedures, it may seem counterintuitive to analyze multiple programs collectively. This Article argues that because big data blacklisting harms have not been legally conceptualized, yet implicate a mass societal harm that threatens fundamental liberty interests, a legal framework that possesses the capacity to analyze and address these new harms collectively is needed. I reserve for future scholarship a more detailed treatment of individual big data blacklisting programs and the application of the due process inquiry more specifically.

Finally, more empirical evidence, programmatic transparency, and evaluative protocols are needed to assess the sources and specific nature of the unreliability of nonclassified and classified or semi-classified government big data programs. To more fully assess the nature of big data blacklisting, further interrogation is necessary to examine the multi-dimensional and significant long-term consequences of the government's increasing reliance on big data policymaking and algorithmic intelligence, and the impact of this reliance on procedural and substantive due process rights.[338] Core liberties may be obstructed in a way that is rapidly evolving and systemic, however, nearly impossible to detect because of the opacity and complexity of big data technologies, and the administrative systems that support them. Consequently, fundamental liberty interests are implicated by big data blacklisting in a way that now necessitates an evolution of the due process jurisprudence.

338. *See, e.g.*, Citron & Pasquale, *The Scored Society*, *supra* note 13, at 27 ("In constructing strategies for technological due process in scoring contexts, it is helpful to consider the sort of notice individuals are owed when governmental systems make adverse decisions about them. Under the Due Process Clause, notice must be 'reasonably calculated' to inform individuals of the government's claims against them.") (citing Dusenbery v. United States, 534 U.S. 161, 168 (2002)); Citron, *Technological Due Process*, *supra* note 28, at 1276–77 ("[A]gencies must recognize and address the ways in which automation undermines the procedural safeguards typically attached to individual adjudications and rulemaking under the Due Process Clauses of the Constitution and federal and state law[.]") (citation omitted); Fairfield & Luna, *supra* note 36, at 994 (arguing in favor of stronger procedural protections for criminal defendants by recognizing the potential exonerating value of Big Data evidence: "What is needed now is . . . an understanding of Big Data and mass government surveillance, and an evaluation of the legal consequences for the actually innocent"); Manta & Robertson, *supra* note 62, at 1 (arguing that "courts should incorporate elements of substantive due process by applying a unified due process standard that requires a higher evidentiary burden—and real evidence of national security benefits—before the government may curtail significant individual liberties").

APPENDICES

Appendix A. Examples of U.S. Citizens Alleging Erroneous Work Opportunity Deprivation from Database Screening

Name	Citizenship	Occupation	Consequences
Juan Carlos Ochoa[339]	Naturalized U.S. Citizen since 2000, Resident of Arizona[340]	Car dealership employee[341]	E-Verify search resulted in an erroneous TNC apparently because the U.S. State Department never notified SSA of his change in status. His employer fired him and his electricity was shut off because he could not pay the bill. Allegedly paid over $400 to secure a new naturalization certificate to clear his name in databases used by the E-Verify database screening system.[342]
Jessica St. Pierre[343]	U.S. Citizen, Resident of Florida[344]	Employee at a telecommunications company[345]	Employment termination due to an E-Verify TNC error that could not be resolved. After three months of unemployment, she attained a new job with "significantly lower pay." Later, with the aid of the National Immigration Law Center, she discovered that the problem occurred allegedly because "the employer had placed two spaces after [her] last name" when entering the information into the E-Verify database screening system.[346]
John Doe I[347]	U.S. Citizen, Resident of Ohio[348]	Former captain in the U.S. Navy with thirty-four years of service[349]	Despite history of high military security clearance, data error required a two-month investigation with the assistance of an attorney to resolve erroneous E-Verify TNC.[350]

339. David Bier, *Why Everyone Should Fear E-Verify*, HUFFINGTON POST (July 13, 2012, 11:57 AM), http://www.huffingtonpost.com/david-bier/why-everyone-should-fear-e-verify_b_1610057.html.

340. *Id.*

341. NAT'L IMMIGRATION LAW CTR., HOW ERRORS IN E-VERIFY DATABASES IMPACT U.S. CITIZENS AND LAWFULLY PRESENT IMMIGRANTS 1 (2011), *available at* http://www.nilc.org/document.html?id=337.

342. *Id.*

343. ACLU, PROVE YOURSELF TO WORK: THE 10 BIG PROBLEMS WITH E-VERIFY (2013), *available at* https://www.aclu.org/files/assets/everify_white_paper.pdf.

344. *Id.*

345. *Id.*

346. *Id.*

347. NAT'L IMMIGRATION LAW CTR., *supra* note 341, at 1, 4 n.2.

348. *Id.*

349. *Id.* at 1.

350. *Id.*

Jane Doe I[351]	U.S. Citizen, Resident of Florida[352]	Employee at a national department store chain[353]	Erroneous E-Verify TNC notice resulted because employee "recently remarried and changed her name." SSA office informed her that the matter was resolved; however, when she returned to work, she was informed that DHS had directed the employer to terminate her employment because employer claimed that the database screening result indicated that "[she was] suspected as a terrorist."[354]
Francisco Romero[355]	Naturalized U.S. Citizen since 1996, Resident of Arizona[356]	Construction worker[357]	Employee fired twice from construction jobs because "E-Verify failed to confirm his employment eligibility." He was "only able to return to work after a community advocate took on his case and located the source of the E-Verify TNC error."[358]
Ken Nagel[359]	U.S. Citizen, Resident of Arizona[360]	Restaurant Owner[361]	Mr. Nagel expressed his concerns over the accuracy of E-Verify after he hired one of his daughters, a native-born U.S. citizen, and upon entering her personally identifiable data into the database screening system, received an erroneous E-Verify TNC regarding her employment eligibility.[362]
Jane Doe II[363]	U.S. Citizen, Resident of Oklahoma[364]	Nursing Home employment applicant[365]	Potential employer rescinded job offer because employee received an erroneous E-Verify TNC, and the nursing home allegedly decided to hire someone else.[366]
Jane Doe III[367]	U.S. Citizen, Resident of California[368]	Searching for a job using an employment services	Informed by an employment agency that there were several employers that would be interested in hiring

351. *Id.* at 2.
352. *Id.*
353. *Id.*
354. *Id.*
355. *Id.*
356. *Id.*
357. *Id.*
358. *Id.*
359. *Id.*
360. *Id.*
361. *Id.*
362. *Id.*
363. *Id.*
364. *Id.*
365. *Id.*
366. *Id.*
367. *Id.*
368. *Id.*

		company[369]	her based on her extensive work history. However, employment agency later informed her that she could not obtain a job because she received an erroneous TNC from E-Verify.[370]
John Doe II[371]	U.S. Citizen, Resident of Colorado[372]	Engineer[373]	Employee received an erroneous TNC and staffing agency revoked job until SSA corrected the error. After SSA corrected the error, the agency could not locate comparable work for the employee.[374]

Appendix B. Examples of U.S. Citizens Claiming Erroneous Voter List Purging Based Upon Database Screening

State	**Criteria Used to Purge Voters**	**General Results of Database Screening**	**Examples of Wrongly Purged U.S. Citizens**
Virginia[375]	State election officials attempted to purge nearly 40,000 voters weeks before election day because names showed up in a database as registered in more than one state.[376]	Of the 38,870 names that were purged, many were later found to be the result of database matching errors. Many voters on the purge list had actually registered in Virginia more recently than the other state. Thus, voters were eligible to vote in Virginia.[377]	"County registrars say hundreds of eligible voters have been removed and complain they've been strong-armed into moving ahead too quickly." Lawrence Haake III, the Chesterfield County registrar and a Republican, joined an affidavit filed by Democrats against the Republican Attorney General, calling the list of 2200 names he had received to be purged "clearly inaccurate and unreliable."[378]
Mississippi[379]	Madison County election commissioner secretly purged more than 10,000	The violation was discovered a week before the Mississippi U.S. presidential	The government removed a Republican congressional candidate in the upcoming election, his wife, and his

369. *Id.*
370. *Id.*
371. *Id.* at 3.
372. *Id.*
373. *Id.*
374. *Id.*
375. Roth, *supra* note 252.
376. *Id.*
377. *Id.*
378. *Id.*
379. PÉREZ, *supra* note 251, at 21.

	residents from voter roll via her home computer based upon database screening.[380]	primary in March 2008. The purge included recent voters in November 2007 elections. The state attempted to correct purge errors before the election.[381]	daughter from the voter rolls.[382]
Georgia[383]	Muscogee County, Georgia, attempted to purge 700 voters from voter rolls because election officials believed purged voters were convicted felons.[384]	Over a third of the 700 voters called to report that the letter they received informing them of the purge was a mistake.[385]	A computer program that matched names of felons to names of voters generated the list used by the county; however, the program used no other identifying information other than the database name to support conclusion that voter was a felon.[386]

Appendix C. Examples of U.S. Citizens Claiming Erroneous Detention, Deportation and Database Screening

Name	Citizenship	Detention or Deportation	Consequences
Mark Lyttle[387]	U.S. citizen born in North Carolina[388]	Lyttle screened through S-COMM database twice. Lyttle filed lawsuit against DHS for wrongful deportation.[389]	Deported to Mexico. Removed from the United States in December of 2008. Crossed border on foot with only three dollars, and wandered through Mexico, Honduras, Nicaragua, and Guatemala for 125 days before being referred to a U.S. consular office that confirmed his citizenship. Lyttle does not speak Spanish.[390]

380. *Id.*
381. *Id.*
382. *Id.*
383. *Id.* at 22.
384. *Id.*
385. *Id.*
386. *Id.*
387. Esha Bhandari, *Yes, the U.S. Wrongfully Deports Its Own Citizens*, ACLU (Apr. 25, 2013, 11:45 AM), https://www.aclu.org/blog/immigrants-rights/yes-us-wrongfully-deports-its-own-citizens.
388. *Id.*
389. *Id.*
390. *Id.*

Jakadrien Turner[391]	U.S. citizen born in Texas[392]	Arrested for shoplifting in Houston, and she gave a false name that matched the name of an undocumented immigrant in the database. Although her fingerprints did not match the false name, the government still deported her.[393]	Deported to Colombia. Turner was fifteen years old at the time of the deportation; lived in Colombia for almost one year before her grandmother located her. Ms. Turner does not speak Spanish.[394]
Antonio Montejano[395]	U.S. Citizen, resident of California[396]	S-COMM led ICE to believe Montejano was an undocumented immigrant.[397] "[I]mmigration officials had failed once before to recognize his citizenship, mistakenly deporting him to Mexico in 1996. His records were not corrected."[398]	Police arrested and charged Montejano with shoplifting. He had purchased $600 worth of merchandise but forgot to pay for candy his children had eaten while in the store and a $10 bottle of perfume that had failed to scan at the register.[399] A Los Angeles county judge ordered his release from jail, but he remained detained due to an immigration hold.[400] Detained for four days in jail by orders of ICE until his citizenship was proven.[401] He was released from prison after the ACLU delivered his passport and birth certificate to ICE.[402]

391. Julianne Hing, *How Did 15-Year-Old Jakadrien Turner, a U.S. Citizen, Get Deported?*, COLORLINES (Jan. 11, 2012, 9:53 AM), http://colorlines.com/archives/2012/01/how_did_jakadrien_turner_a_us_citizen_get_deported.html.

392. *Id.*

393. *Id.*

394. *Id.*

395. E.J. Tamara, *Secure Communities Program Arrested U.S. Citizens: Report*, HUFFINGTON POST (Dec. 15, 2011, 10:37 AM), http://www.huffingtonpost.com/2011/12/15/secure-communities-us-citizens-arrested_n_1150877.html; *see also* Keith Rushing, *SCOMM Leads to Jailing of Another U.S. Citizen*, RIGHTS WORKING GRP. (Dec. 16, 2011, 11:58 AM), http://www.rightsworkinggroup.org/content/scomm-leads-jailing-another-us-citizen.

396. Tamara, *supra* note 395.

397. *Id.*

398. Julia Preston, *Immigration Crackdown Also Snares Americans*, N.Y. TIMES (Dec. 13, 2011), http://www.nytimes.com/2011/12/14/us/measures-to-capture-illegal-aliens-nab-citizens.html.

399. Tamara, *supra* note 395.

400. *Id.*

401. Simone Wilson, *Antonio Montejano, U.S. Citizen and L.A. Dad, Detained for Days on 'Immigration Hold,'* LA WEEKLY (Dec. 14, 2011), http://www.laweekly.com/informer/2011/12/14/antonio-montejano-us-citizen-and-la-dad-detained-for-days-on-immigration-hold.

402. Tamara, *supra* note 395.

James Makowski[403]	Makowski became a naturalized U.S. citizen at the age of one, but the government did not update his immigration records, according to his lawyer.[404] Born in India and adopted by a U.S. family when he was four months old.[405]	S-COMM led ICE to believe Makowski was anundocumented immigrant.[406]	Makowski was "incorrectly identified . . . as an illegal immigrant and authorities ordered him detained in a maximum-security prison."[407] Detained for two months. "Mr. Makowski was accepted into the U.S. Marines in 2004 and underwent an FBI check as part of that process. Nevertheless, DHS never updated its records to reflect Mr. Makowski's citizenship."[408] Filed lawsuit against the FBI and DHS.[409]
Jose Velazquez[410]	U.S. citizen[411]	S-COMM led ICE to believe Velasquez was an undocumented immigrant.[412]	U.S. citizen wrongfully detained in Los Angeles County.[413]
Romy Campos[414]	Dual citizen of United States and Spain, born in Florida[415]	Once entered the U.S. on her Spanish passport, which triggered the S-COMM database.[416]	Nineteen-year-old college student who spent four days in jail on an immigration detainer following a misdemeanor charge.[417]

403. *U.S. Citizen Sues FBI and DHS for Unlawful Imprisonment Due to Secure Communities*, NAT'L IMMIGRANT JUSTICE CTR. (July 3, 2012), http://www.immigrantjustice.org/press_releases/us-citizen-sues-fbi-and-dhs-unlawful-imprisonment-due-secure-communities [hereinafter *U.S. Citizen Sues*].

404. *Id.*

405. Brian Bennett, *Citizen Sues over Imprisonment Under Fingerprint-Sharing Program*, L.A. TIMES (July 6, 2012), http://articles.latimes.com/2012/jul/06/nation/la-na-secure-communities-20120706.

406. *Id.*

407. *Id.*

408. *U.S. Citizen Sues*, *supra* note 403.

409. *Id.*

410. Velasquez was reportedly going to join Antonio Montejano in a lawsuit over their incarceration. *See* Tamara, *supra* note 395.

411. *Id.*

412. *See id.*

413. *Id.*

414. Preston, *supra* note 398.

415. *Id.*

416. *Id.*

417. *Id.*

Andres Robles[418]	U.S. citizen that acquired derived citizenship when his father, a U.S. citizen, was naturalized in 2002.[419]	Law enforcement paperwork allegedly contained errors, possibly leading to a positive match in S-COMM.[420]	Deported to Mexico in 2011.[421] Received a letter in Mexico stating that the U.S. government would issue a certificate of citizenship; however, was required to retrieve letter in person in the United States. He was unable to do so because he was erroneously deported. Filed lawsuit against DHS.[422]
Geraldo Gonzales, Jr. [423]	U.S. citizen born in California[424]	When arrested in December 2012 on a drug charge, arrest report erroneously stated he was born in Mexico.[425]	When he became eligible for release from drug charge, he attempted to post bail and learned that he was on an immigration hold by ICE, despite ICE's lack of authority to detain U.S. citizens.[426]
Hector Veloz[427]	Born in Mexico, but U.S. citizen by birth: father is a U.S. citizen who was serving in Vietnam, mother went to stay at family's house in Mexico while she was pregnant.[428]	Arrested in 2006 when he bought a stolen car. ICE did not believe he was a U.S. citizen because his parents had never obtained a certificate of citizenship for him.[429]	After nine months in jail, an Arizona judge declared that he was a U.S. citizen and ordered release. ICE appealed the ruling, and he remained in jail for five more months.[430]

418. Alex Nowrasthe, *Commentary: Mistaken Deportation of Texas Teen Highlights the Rigid, Incompetent Immigration Bureaucracy*, HOUS. CHRON. BLOG (Jan. 6, 2012), http://blog.chron.com/txpotomac/2012/01/commentary-mistaken-deportation-of-texas-teen-highlights-the-rigid-incompetent-immigration-bureaucracy/.

419. *Id*.

420. *See* Jacqueline Stevens, *How ICE Deported Another U.S. Citizen, Andres Robles Still in Mexico*, STATES WITHOUT NATIONS BLOG (July 27, 2011, 1:15 PM), http://stateswithoutnations.blogspot.com/2011/07/how-ice-deported-another-us-citizen.html.

421. Nowrasthe, *supra* note 418.

422. *Id.*

423. Aura Bogado, *Why Is This US-Born Citizen Being Detained by ICE?*, NATION (June 21, 2013, 10:52 AM), http://www.thenation.com/blog/174921/why-us-born-citizen-being-detained-ice#.

424. *Id*.

425. *Id.*

426. *Id.*

427. Tyche Hendricks, *U.S. Citizens Wrongly Detained, Deported by ICE*, SF GATE (July 27, 2009, 4:00 AM), http://www.sfgate.com/news/article/U-S-citizens-wrongly-detained-deported-by-ICE-3291041.php.

428. *Id*.

429. *Id*.

430. *Id*.

Jhon Erik Ocampo[431]	U.S. citizen, derived citizenship in 2002 from his mother's naturalization[432]	No explanation for the mistaken detention.[433]	ICE came to Ocampo's home and arrested him, reportedly based on database hit after he had been convicted of other crimes. Despite providing necessary documentation to prove citizenship, including his mother's naturalization information, detained for several days.[434]

Appendix D. Examples of U.S. Citizens and Lawful Immigrants Challenging Erroneous Placement on No Fly List Based upon Digital Watchlisting and Database Screening[435]

Name	**State**	**Occupation**	**Consequences**
Ibraheim (Abe) Mashal[436]	Illinois[437]	U.S. Marine Corps veteran and owner of a dog training business[438]	Lost business clients due to his inability to fly. Unable to travel to family events such as his sister-in-law's graduation and to fundraising events for the nonprofit organization that he founded. [439]
Amayan Latif[440]	Georgia[441]	U.S. Marine Corps veteran[442]	Lost his veteran disability benefits because he could not attend scheduled evaluations required for benefits.[443]
Mohamed Sheikh Abdirahman Kariye[444]	Oregon[445]	N/A	Could not fly to visit his daughter who is studying in Dubai and cannot fly to accompany his mother on a *hajj* pilgrimage.[446]

431. *See* Jacqueline Stevens, *ICE Kidnaps Another US Citizen in Springfield, Illinois*, STATES WITHOUT NATIONS BLOG (June 21, 2012, 12:15 PM), http://stateswithoutnations.blogspot.com/2012/06/ice-kidnaps-another-us-citizen-in.html.

432. *Id*.

433. *See id*.

434. *Id*.

435. In 2012, according to a spokesman for the TSC, the number of U.S. citizens on the list remains "'very small' and relatively stable, at 500." Stone, *supra* note 297.

436. *Federal Court Sides with ACLU in No Fly List Lawsuit*, ACLU (Aug. 29, 2013), https://www.aclu.org/national-security/federal-court-sides-aclu-no-fly-list-lawsuit.

437. *Id.*

438. *Id.*

439. *See id.*

440. Latif v. Holder, 969 F. Supp. 2d 1293, 1298 (D. Or. 2013).

441. *Id.*

442. *Id.*

443. *Id.* Latif was unable to return to the United States and remained in Egypt for six months because the government did not allow him to board a flight home. *Id.* In October 2010, the Egyptian government granted him a "one-time waiver" to fly to the United States. *Id.*

444. *Id.* at 1298–99.

445. *Id.*

446. *Id.*

Raymond Earl Knaeble IV[447]	Illinois[448]	U.S. Army veteran[449]	Job offer rescinded because he was unable to fly home for required medical examination. Prevented from returning home after visiting his wife's family in Columbia. Eventually resorted to traveling for twelve days through Mexico to California to return home.[450]
Steven William Washburn[451]	New Mexico[452]	U.S. Air Force veteran[453]	Returned to United States by taking a series of five flights from Ireland to Mexico, and then by crossing the U.S. border on foot. Unable to see wife since May 2010 because she is unable to obtain a visa to fly to the United States.[454]
Salah Ali Ahmed[455]	Georgia[456]	N/A	Unable to travel to Yemen in 2012 to attend brother's funeral and cannot visit his extended family.[457]
Amir Meshal[458]	Minnesota[459]	N/A	Could not visit his mother and extended family in Egypt. Allegedly offered the opportunity to serve as an informant in exchange for removal from the No Fly List.[460]
Stephen Durga Persaud[461]	California[462]	N/A	Five-day boat trip from St. Thomas to Miami and a four-day train ride from Miami to Los Angeles to be present for the birth of his second child. Cannot travel to perform *hajj* pilgrimage.[463]

447. *Id.* at 1299.
448. *Id.*
449. *Id.*
450. *Id.*
451. *Id.* at 1299–1300.
452. *Id.*
453. *Id.*
454. *Id.*
455. *Id* at 1301.
456. *Id.*
457. *Id.*
458. *Id.*
459. *Id.*
460. *Id.*
461. *Id.*
462. *Id.*
463. *Id.*

Yahye Wehelie[464]	Virginia[465]	Student who studied in Yemen for eighteen months[466]	Questioned in Egypt for six weeks before receiving a one-time waiver to return home. The Virginia native reported that the FBI asked him to be an informant in the Muslim American community.[467]
Kevin Iraniha[468]	California[469]	Student with a masters degree in International Law[470]	Prevented from flying home from his graduate studies in Costa Rica. Forced to travel to Mexico and cross into the United States by land. After questioning, the FBI allegedly asked him to be an informant.[471]
Muhammed Tanvir[472]	New York[473]	Lawful permanent resident[474]	Allegedly offered the opportunity to serve as an informant in exchange for removal from the No Fly List.[475]

464. Ian Shapira, *U.S. Citizen on No-Fly List Discusses Being Stranded in Egypt and Talks with FBI*, WASH. POST (July 27, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/07/26/AR2010072605404.html.

465. *Id.*

466. *Id.*

467. *Id.*

468. Shirin Sadeghi, *U.S. Citizen Put on No-Fly List to Pressure Him into Becoming FBI Informant*, HUFFINGTON POST (June 7, 2012, 12:00 AM), http://www.huffingtonpost.com/shirin-sadeghi/kevin-iraniha-no-fly-list_b_1579208.html.

469. *Id.*

470. *Id.*

471. *Id.*

472. Hunter Stuart, *Muhammed Tanvir, New York Man, Put on No-Fly List After Refusing to Spy for FBI, Lawsuit Says*, HUFFINGTON POST (Oct. 7, 2013, 11:05 AM), http://www.huffingtonpost.com/2013/10/04/fbi-spy-no-fly-list-lawsuit-muslims-_n_4045791.html.

473. *Id.*

474. *Id.*

475. *Id.*