Fordham Law Review

Volume 86 | Issue 2 Article 13

2017

# Algorithmic Jim Crow

Margaret Hu
*Washington and Lee University School of Law*

# ARTICLES

# ALGORITHMIC JIM CROW

*Margaret Hu**

*This Article contends that current immigration- and security-related vetting protocols risk promulgating an algorithmically driven form of Jim Crow. Under the "separate but equal" discrimination of a historic Jim Crow regime, state laws required mandatory separation and discrimination on the front end, while purportedly establishing equality on the back end. In contrast, an Algorithmic Jim Crow regime allows for "equal but separate" discrimination. Under Algorithmic Jim Crow, equal vetting and database screening of all citizens and noncitizens will make it appear that fairness and equality principles are preserved on the front end. Algorithmic Jim Crow, however, will enable discrimination on the back end in the form of designing, interpreting, and acting upon vetting and screening systems in ways that result in a disparate impact.*

*Currently, security-related vetting protocols often begin with an algorithm-anchored technique of biometric identification—for example, the collection and database screening of scanned fingerprints and irises, digital photographs for facial recognition technology, and DNA. Immigration reform efforts, however, call for the biometric data collection of the entire citizenry in the United States to enhance border security efforts and to increase the accuracy of the algorithmic screening process. Newly*

* Associate 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: Sahar Aziz, Jack Balkin, Kate Bartlett, Gerlinde Berger-Walliser, Joseph Blocher, danah boyd, Devon Carbado, Jennifer Chacón, Guy Charles, Andrew Christensen, Danielle Citron, Adam Cox, Deven Desai, Mark Drumbl, Michelle Drumbl, Josh Fairfield, Frank Pasquale, Jennifer Granick, Janine Hiller, Gordon Hull, Trina Jones, Stephen Lee, Charlton McIlwain, Steve Miskinis, Hiroshi Motomura, Kish Parella, Jeff Powell, Angie Raymond, Bertrall Ross, Victoria Sahani, Andrew Selbst, and Kevin Werbach. In addition, this research benefited greatly from the discussions generated from the Immigration Law Professors Workshop; the Law & Society Association Annual Meeting; Yale Law School's Information Society Project's Unlocking the Black Box Conference; the Privacy Law Scholars Conference; Data & Society Research Institute's Eclectic Paper Workshop; Duke Law School's Culp Colloquium; Texas A&M Faculty Workshop Series; UNC Charlotte Surveillance Colloquium; and the Wharton School of the University of Pennsylvania, Law & Ethics of Big Data Colloquium. Many thanks to the editorial care of Vincent Margiotta of the *Fordham Law Review*, and for the generous research assistance of Alexandra Klein, Kirby Kreider, Bo Mahr, and Carroll Neale. All errors and omissions are my own.

*developed big data vetting tools fuse biometric data with biographic data and internet and social media profiling to algorithmically assess risk.*

*This Article concludes that those individuals and groups disparately impacted by mandatory vetting and screening protocols will largely fall within traditional classifications—race, color, ethnicity, national origin, gender, and religion. Disparate-impact consequences may survive judicial review if based upon threat risk assessments, terroristic classifications, data-screening results deemed suspect, and characteristics establishing anomalous data and perceived foreignness or dangerousness data—nonprotected categories that fall outside of the current equal protection framework. Thus, Algorithmic Jim Crow will require an evolution of equality law.*



## INTRODUCTION

During the 2016 presidential campaign, then-candidate Donald J. Trump announced his intention to impose a "Muslim Ban," which would prohibit Muslim entry into the United States[1] as part of his counterterrorism strategy.

1. *See, e.g.*, Jeremy Diamond, *Donald Trump: Ban All Muslim Travel to U.S.*, CNN (Dec. 8, 2015, 4:18 AM), http://www.cnn.com/2015/12/07/politics/donald-trump-muslim-ban-immigration/ [https://perma.cc/L3D4-UMHX]. Immigration, constitutional, and national security experts have offered perspectives on the ongoing legal challenges surrounding the Travel Ban. *See generally* Margaret Hu, *Crimmigration-Counterterrorism and the Travel Ban*, 2017 WIS. L. REV. (forthcoming) (citing Adam Cox, *Why a Muslim Ban Is Likely to Be Held Unconstitutional: The Myth of Unconstrained Immigration Power*, JUSTSECURITY (Jan.

Shortly before his election, Trump also announced a proposal for the "extreme vetting" of immigrants and refugees.[2] Trump clarified that "[t]he Muslim ban is something that in some form has morphed into a[n] extreme vetting [protocol] from certain areas of the world."[3]

On January 27, 2017, during his first week as president, Trump signed Executive Order 13,769, titled "Protecting the Nation from Foreign Terrorist Entry into the United States" (the "January 27, 2017, Order").[4] Litigation concerning the constitutionality of this Executive Order[5] focused on sections 3 and 5(c), provisions that relate to barring the entry of travelers and refugees from specific Muslim-majority countries into the United States.[6] These controversial provisions were challenged as violating equal protection, due process, and the Establishment Clause of the First Amendment, among other constitutional and statutory claims.[7]

On March 6, 2017, President Trump issued a revised Executive Order (the "March 6 2017, Order"), Executive Order 13,780. Issued under the same title as the January 27, 2017, Order, "Protecting the Nation from Foreign Terrorist Entry into the United States," the March 6, 2017, Order superseded the

---

30, 2017, 10:21 AM), https://www.justsecurity.org/36988/muslim-ban-held-unconstitutional-myth-unconstrained-immigration-power/ [https://perma.cc/H234-52N2]; then citing Mark Tushnet, *Mootness and the Travel Ban*, BALKINIZATION (June 2, 2017, 1:18 AM) https://balkin.blogspot.com/2017/06/mootness-and-travel-ban.html [https://perma.cc/2LNR-J67T]; then citing Marty Lederman, *Unlocking the Mysteries of the Supreme Court's Entry Ban Case*, JUSTSECURITY (June 27, 2017, 8:01 PM), https://www.justsecurity.org/42577/mysteries-trump-v-irap/ [https://perma.cc/JAM4-D97M]; and then citing Leah Litman & Steve Vladeck, *How the President's "Clarifying" Memorandum Destroys the Case for the Entry Ban*, JUSTSECURITY (June 15, 2017, 8:01 AM), https://www.justsecurity.org/42166/presidents-clarifying-memorandum-destroys-case-entry-ban/ [https://perma.cc/6APK-MZGL]).

2. Gerhard Peters & John T. Wooley, *Presidential Debate at Washington University in St. Louis, Missouri*, AM. PRESIDENCY PROJECT (Oct. 9, 2016), http://www.presidency.ucsb.edu/ws/index.php?pid=119038 [https://perma.cc/A79V-TLVW]; *see also* Peter Margulies, *Bans, Borders, and Justice: Judicial Review of Immigration Law in the Trump Administration* at 35–48 (Roger Williams Univ. Sch. of Law, Research Paper No. 177, 2017), http://ssrn.com/abstract=3029655 [https://perma.cc/E5DP-UDQQ] (arguing for a more searching judicial review of "extreme vetting" and the need to recognize the significant long-term impact of "extreme vetting").

3. Peters & Wooley, *supra* note 2.

4. Exec. Order No. 13,769, 82 Fed. Reg. 8977 (Feb. 1, 2017) [hereinafter January 27, 2017, Order].

5. *See, e.g.*, Washington v. Trump, 847 F.3d 1151, 1157 (9th Cir. 2017) (per curiam).

6. January 27, 2017, Order, *supra* note 4, §§ 3, 5(c).

7. *See, e.g.*, Hawaii v. Trump, 859 F.3d 741, 760 (9th Cir.) (per curiam) (alleging violations of the Establishment Clause, the Equal Protection and Due Process Clauses of the Fifth Amendment (both procedural and substantive claims), the Immigration and Nationality Act, the Religious Freedom Restoration Act, and the Administrative Procedure Act), *cert. granted*, 137 S. Ct. 2080 (2017); Int'l Refugee Assistance Project v. Trump, 857 F.3d 554, 578–79 (4th Cir.) (claiming violations of the Equal Protection Clause of the Fifth Amendment, the Immigration and Nationality Act, the Religious Freedom Restoration Act, the Refugee Act, and the Administrative Procedure Act), *cert. granted*, 137 S. Ct. 2080 (2017); *Washington*, 847 F.3d at 1157, 1165, 1167 (alleging that the Executive Order violates that First Amendment's Establishment Clause, due process, and equal protection); Darweesh v. Trump, 17 Civ. 480 (AMD), 2017 WL 388504 (E.D.N.Y. Jan. 28, 2017) (alleging that the Executive Order violates the Equal Protection and Due Process Clauses).

January 27, 2017, Order.[8] However, it left the extreme vetting provisions of the January 27, 2017, Order in place,[9] and, in fact, expanded the vetting requirements in several respects.[10] The extreme vetting requirements of the March 6, 2017, Order are now most fully articulated in section 5, titled "Implementing Uniform Screening and Vetting Standards for All Immigration Programs."[11]

The travel restrictions and the vetting requirements were expanded yet again in a third iteration of the "Muslim Ban," also referred to as the "Travel Ban" or the "Entry Ban." On September 24, 2017, shortly before oral argument was scheduled for the U.S. Supreme Court on October 10, 2017, in the consolidated Travel Ban cases of *Trump v. Hawaii* and *Trump v. International Refugee Assistance Project*,[12] President Trump signed a new Proclamation (the "September 24, 2017, Order").[13] The September 24, 2017, Order is titled, "Enhancing Vetting Capabilities and Processes for Detecting Attempted Entry into the United States by Terrorists or Other Public-Safety Threats."[14] Thus, the most recent Order, as implied by the title, focuses more squarely on the extreme vetting provisions set forth by the prior Orders. More specifically, sections 1(a) through (h) of the September 24, 2017, Order focus on "identity-management and information-sharing capabilities, protocols, and practices" related to immigration screening and vetting.[15] The next day, the Court ordered briefing as to whether the Travel Ban cases that had been scheduled for oral argument on October 10, 2017, were moot.[16] At the time of publication, the litigation remains ongoing, including challenges to the September 24, 2017, Order.[17]

---

8. Exec. Order No. 13,780, 82 Fed. Reg. 13,209 (Mar. 6, 2017) [hereinafter March 6, 2017, Order].

9. *Id.* §§ 1–2; *see also id.* § 5 ("Implementing Uniform Screening and Vetting Standards for All Immigration Programs").

10. *Compare id.*, *with* January 27, 2017, Order, *supra* note 4, § 4.

11. March 6, 2017, Order, *supra* note 8, § 5.

12. 137 S. Ct. 2080 (2017).

13. Presidential Proclamation, Enhancing Vetting Capabilities and Processes for Detecting Attempted Entry into the United States by Terrorists or Other Public-Safety Threats (Sept. 24, 2017) [hereinafter "September 24, 2017, Order"], https://www.whitehouse.gov/the-press-office/2017/09/24/enhancing-vetting-capabilities-and-processes-detecting-attempted-entry [https://perma.cc/R678-KL5F].

14. *Id.*

15. *Id.*; *see also infra* note 50 and accompanying text (discussing U.S. Department of Homeland Security definition of "identity management").

16. Trump v. Int'l Refugee Assistance Project, Nos. 16-1436, 16-1540, slip op. (U.S. Sept. 25, 2017), https://www.supremecourt.gov/orders/courtorders/092517zr_jiel.pdf [https://perma.cc/24F6-5MFB] (ordering parties to file letter briefs addressing whether, or to what extent, the Proclamation issued on September 24, 2017, may render the consolidated cases moot).

17. *See, e.g.*, Complaint for Declaratory and Injunctive Relief at 26–27, Iranian Alliances Across Borders, Univ. of Md. Coll. Park Chapter v. Trump, No. 8:17-cv-02921-GJH (D. Md. Oct. 2, 2017) (seeking declaratory and injunctive relief from the September 24, 2017, Order and alleging that the Order violates the antidiscrimination provision of the Immigration and Nationality Act, 8 U.S.C. § 1152(a)(1)(A) (2012)); Letter from ACLU to Hon. Theodore D. Chuang, U.S. Dist. Ct. for the Dist. of Md. (Sept. 29, 2017), https://www.aclu.org/letter/irap-v-trump-pmc-letter [https://perma.cc/KKL8-DM8W] (seeking to amend the complaint in *International Refugee Assistance Project* in light of the September 24, 2017, Order); s*ee also*

Regardless of the final disposition of these litigation matters, it is significant to note that the extreme vetting provisions of the original and revised Executive Orders have received less judicial attention than the travel restrictions.[18] The extreme vetting provisions do not appear to be dependent upon the authority of the Orders, and are presented in the Orders as an evolving and prospective administrative matter.[19] Thus, the vetting provisions of the March 6, 2017, Order and the September 24, 2017, Order may not be fully challenged.[20]

This Article focuses on the long-term impact of modern vetting requirements, such as those prescribed in the Executive Orders referenced above,[21] and other immigration-related screening protocols that are increasingly algorithmically anchored. It contends that the implementation of expanded vetting protocols[22] risks implications that may be undertheorized due to an underappreciation of the mass cybersurveillance and disparate-impact consequences that surround current screening measures broadly promulgated by the U.S. Department of Homeland Security (DHS). Specifically, this Article advances the claim that DHS vetting and screening

---

Complaint for Declaratory and Injunctive Relief at 1, Brennan Ctr. for Justice at N.Y. Univ. Sch. of Law v. U.S. Dep't. of State, No. 1:17-cv-07520 (S.D.N.Y. Oct. 2, 2017) (seeking disclosure of reports referred to in sections 1(c) and 1(h) of the September 24, 2017, Order, pursuant to the disclosure requirements of the Freedom of Information Act, 5 U.S.C. § 552 (2012)).

18. Litigation surrounding the March 6, 2017, Order addressed sections 2 and 6, which bar the entry of travelers from six designated countries and limit refugee admissions. *See Hawaii*, 859 F.3d at 757–59; *Int'l Refugee Assistance Project*, 857 F.3d at 574–75.

19. The implementation of "extreme vetting" measures appears to be underway. *See* Notice of Modified Privacy Act System of Records, 82 Fed. Reg. 179 (Sept. 18, 2017); 60-Day Notice of Proposed Information Collection: Supplemental Questions for Visa Applicants, 82 Fed. Reg. 148 (Aug. 3, 2017).

20. *See, e.g.*, Hu, *supra* note 1; Margulies, *supra* note 2. Increasing attention has been focused on the efficacy of the social media screening of immigration vetting protocols. *See, e.g.*, OFFICE OF INSPECTOR GEN., DEP'T OF HOMELAND SEC., OIG-17-40, DHS' PILOTS FOR SOCIAL MEDIA SCREENING NEED INCREASED RIGOR TO ENSURE SCALABILITY AND LONG-TERM SUCCESS (2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf [https://perma.cc/5ACP-GU2G]; Lily Hay Newman, *Feds Monitoring Social Media Does More Harm Than Good*, WIRED (Sept. 28, 2017, 8:00 AM), https://www.wired.com/story/dhs-social-media-immigrants-green-card/ [https://perma.cc/2FC5-FPKC].

21. January 27, 2017, Order, *supra* note 4, § 4; March 6, 2017, Order, *supra* note 8, § 5; September 24, 2017, Order, *supra* note 13, § 1(a)-(h).

22. As a presidential candidate, Trump announced his plans to implement a program of "extreme vetting" of immigrants and refugees in a campaign speech on the Islamic State of Iraq and Syria (ISIS) in August 2016. *See* Jeremy Diamond, *Trump Proposes Values Test for Would-Be Immigrants in Fiery ISIS Speech*, CNN (Aug. 15, 2016, 9:39 PM) http://www.cnn.com/2016/08/14/politics/donald-trump-isis-fight/index.html [https://perma.cc/8GU4-9AEK]. Several scholars have observed that the president enjoys wide powers in the exercise of immigration law and policy, especially through executive action. *See, e.g.*, Adam B. Cox & Cristina M. Rodríguez, *The President and Immigration Law*, 119 YALE L.J. 458, 500 (2009); Adam B. Cox & Cristina M. Rodríguez, *The President and Immigration Law Redux*, 125 YALE L.J. 104, 108 (2015).

protocols risk introducing an algorithmically driven and technologically enhanced form of Jim Crow.[23]

Unlike the "separate but equal"[24] de jure discrimination[25] of a historic Jim Crow regime, Algorithmic Jim Crow risks imposing both de jure and de facto discrimination[26] through an "equal but separate"[27] regime. This Article explains how Algorithmic Jim Crow is an outgrowth of a digital era that

23. *See generally* JONATHAN SCOTT HOLLOWAY, JIM CROW WISDOM: MEMORY AND IDENTITY IN BLACK AMERICA SINCE 1940 (2013); JUMPIN' JIM CROW: SOUTHERN POLITICS FROM CIVIL WAR TO CIVIL RIGHTS (Jane Dailey et al. eds., 2000); Mattias Smångs, *Doing Violence, Making Race: Southern Lynching and White Racial Group Formation*, 121 AM. J. SOC. 1329 (2016). For contemporary discussions on the complexity of what has been termed a "post-racial" America, see generally DEVON W. CARBADO & MITU GULATI, ACTING WHITE? RETHINKING RACE IN "POST-RACIAL" AMERICA (2013); THE NEW BLACK: WHAT HAS CHANGED—AND WHAT HAS NOT—WITH RACE IN AMERICA (Kenneth W. Mack & Guy-Uriel E. Charles eds., 2013); Charlton McIlwain, *Racial Formation, Inequality and the Political Economy of Web Traffic*, 20 INFO. COMM. & SOC'Y 1073 (2016); Angela Onwuachi-Willig, *Policing the Boundaries of Whiteness: The Tragedy of Being "Out of Place" from Emmett Till to Trayvon Martin*, 102 IOWA L. REV. 1113 (2017); Camille Gear Rich, *Marginal Whiteness*, 98 CALIF. L. REV. 1497 (2010); *infra* Part I.A.

24. Plessy v. Ferguson, 163 U.S. 537, 550–51 (1896), *overruled by* Brown v. Bd. of Educ., 347 U.S. 483 (1954) ("[W]e cannot say that a law which authorizes or even requires the separation of the two races in public conveyances is unreasonable . . . .").

25. The Supreme Court has characterized de jure discrimination as encompassing state-sanctioned or state-imposed discrimination under the law, prohibited under the Equal Protection Clause. *See, e.g.*, *Brown*, 347 U.S. at 490 (explaining that the Fourteenth Amendment "proscrib[es] all state-imposed discriminations against the Negro race").

26. Nonracial classifications that result in de facto discrimination or disparate-impact discrimination may not be found to violate the Equal Protection Clause. *See, e.g.*, Village of Arlington Heights v. Metro. Hous. Dev. Corp., 429 U.S. 252, 270 (1977) (explaining that the party asserting an equal protection violation bears the burden to show that the governmental action was intended to discriminate against a suspect or protected class); Milliken v. Bradley, 418 U.S. 717, 745 (1974) (distinguishing de jure and de facto segregation with express and explicit policies that articulate race-based distinctions defined as de jure discrimination); *see also* Frank I. Goodman, *De Facto School Segregation: A Constitutional and Empirical Analysis*, 60 CALIF. L. REV. 275, 275 (1972); Richard A. Primus, *Equal Protection and Disparate Impact: Round Three*, 117 HARV. L. REV. 494, 496–97 (2003).

27. *See infra* Part III.A.

exploits cybersurveillance[28] and dataveillance[29] systems that are rapidly proliferating in both the public[30] and private sectors.[31]

This Article demonstrates how immigration-related vetting and database screening protocols utilize newly developed big data[32] screening, tracking, and profiling tools that attempt to verify identity and assess future risk.[33] These tools are now actively deployed by DHS[34] and utilize databases

28. *See, e.g.*, LAWRENCE LESSIG, CODE VERSION 2.0, at 209 (2006) ("[Cybersurveillance is] 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.").

29. *See generally* Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 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: AN OVERVIEW 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 . . . .").

30. *See, e.g.*, GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 6 (2014). *See generally* SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX (2014); LYON, *supra* note 29; DANA PRIEST & WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE (2011); JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE (2005); Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579 (2014); Anil Kalhan, *Immigration Surveillance*, 74 MD. L. REV. 1 (2014); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269 (2012); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

31. *See, e.g.*, JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 17–18 (2014); ROBERT O'HARROW, JR., NO PLACE TO HIDE, 221–23 (2005); *see also* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 596 (2004); Jeffrey Rosen, *The Deciders: Facebook, Google, and the Future of Privacy and Free Speech*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 69, 69–72 (Jeffrey Rosen & Benjamin Wittes eds., 2011).

32. *See generally* ROB KITCHIN, THE DATA REVOLUTION: BIG DATA, OPEN DATA, DATA INFRASTRUCTURES & THEIR CONSEQUENCES (2014); VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013); PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT (Julia Lane et al. eds., 2014).

33. *See, e.g.*, DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST)/PASSIVE METHODS FOR PRECISION BEHAVIORAL SCREENING 5 (2011), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast-a.pdf [https://perma.cc/YQ4W-VM5P].

34. *See, e.g.*, *Refugee Processing and Security Screening*, U.S. CITIZENSHIP & IMMIGR. SERVICES (Dec. 3, 2015), https://www.uscis.gov/refugeescreening [https://perma.cc/4Z6R-C3QQ].

operated by the military[35] and intelligence communities.[36] Currently, vetting and screening protocols often begin with biometric identification[37]—for example, the digital collection and screening of scanned fingerprints through federal and state biometric databases in the United States and international biometric databases, such as those operated by ICPO-INTERPOL (Interpol).[38] Biometric data currently collected by DHS include scanned fingerprints[39] and irises,[40] digital photos for facial recognition technology,[41] and DNA.[42]

Consequently, implementation of extreme vetting protocols will likely include proposals for a tamper-resistant and fraud-proof biometric electronic identity card,[43] such as a biometric ePassport.[44] The Trump administration's Executive Orders, for example, specifically mandate "Expedited Completion of the Biometric Entry-Exit Tracking System" by DHS.[45] As part of new

35. Current refugee vetting procedures include database screening through the U.S. Department of Defense's Defense Forensics and Biometrics Agency's (DFBA) Automated Biometric Identification System (ABIS). *Id.* ("A biometric record check of the Department of Defense's (DOD) records collected in areas of conflict (predominantly Iraq and Afghanistan). DOD screening began in 2007 for Iraqi applicants and has now been expanded to all nationalities.").

36. Current refugee vetting procedures include database screening through the "National Counterterrorism Center/Terrorist Screening Center (terrorist watch lists)" and the "FBI Fingerprint Check through Next Generation Identification (NGI)." *Id.*

37. Biometrics is "[t]he science of automatic identification or identity verification of individuals using physiological or behavioral characteristics." JOHN VACCA, BIOMETRIC TECHNOLOGIES AND VERIFICATION SYSTEMS 589 (2007).

38. *See Databases*, INTERPOL, https://www.interpol.int/INTERPOL-expertise/Databases [https://perma.cc/RVM3-JKJ6] (last visited Oct. 16, 2017).

39. *See, e.g.*, DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT) 15 (2012), https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_usvisit_ident_appendixj_jan2013.pdf [https://perma.cc/2LW4-PJSS]; *Office of Biometric Identity Management Identification Services*, DEP'T HOMELAND SECURITY, https://www.dhs.gov/obim-biometric-identification-services [https://perma.cc/VN5T-H6UH] (last visited Oct. 16, 2017).

40. *See, e.g.*, DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE IRIS AND FACE TECHNOLOGY DEMONSTRATION AND EVALUATION (IFTDE) 2 (2010), https://www.dhs.gov/sites/default/files/publications/privacy_pia_st_iftde.pdf [https://perma.cc/A9MP-CRCF].

41. *See, e.g.*, DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR THE STANDOFF TECHNOLOGY INTEGRATION AND DEMONSTRATION PROGRAM: BIOMETRIC OPTICAL SURVEILLANCE SYSTEM TESTS 2 (2012), https://www.dhs.gov/sites/default/files/publications/privacy_pia_st_stidpboss_dec2012.pdf [https://perma.cc/L7XK-EDK9].

42. *See, e.g.*, DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE RAPID DNA SYSTEM 2 (2013), https://www.dhs.gov/sites/default/files/publications/privacy-pia-rapiddna-20130208.pdf [https://perma.cc/K9NN-F4PL].

43. *See, e.g.*, Charles E. Schumer & Lindsey O. Graham, *The Right Way to Mend Immigration*, WASH. POST (Mar. 19, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/03/17/AR2010031703115.html [https://perma.cc/Y5GF-WE2M] ("We would require all U.S. citizens and legal immigrants who want jobs to obtain a high-tech, fraud-proof Social Security card. Each card's unique biometric identifier would be stored only on the card . . . .").

44. *See, e.g.*, Eric Markowitz, *Retina Scanners and Biometric Passports: A Look at the Futuristic Tech That Could Scan Refugees*, INT'L BUS. TIMES (Nov. 25, 2015, 11:29 AM), http://www.ibtimes.com/retina-scanners-biometric-passports-look-futuristic-tech-could-scan-refugees-2199960 [https://perma.cc/6AZC-3EV9].

45. March 6, 2017, Order, *supra* note 8, § 8; January 27, 2017, Order, *supra* note 4, § 7.

vetting protocols, DHS also seeks social media identification data[46] and plans to seek social media user credentials,[47] such as passwords to Facebook accounts of refugees and visa applicants.[48] Newly developed "big data" cybersurveillance tools fuse biometric data with biographic data and internet and social media profiling to assess risk.[49]

This Article aims to explain how big data vetting is mistakenly presented as a procedure that is restricted to noncitizens: immigrants, refugee and asylum applicants, and visitors seeking a travel visa to the United States. Instead, such vetting is part of a web of technologies that DHS has termed "identity management."[50] The application of these technologies may eventually extend to the entire citizenry through a variety of policy proposals, including a biometric national identification system, and various mandatory vetting and database screening programs. Identity-management programs attempt to authenticate identity and assess the risk factors across entire populations, including the U.S. citizenry. Big data vetting, thus, is misunderstood as a protocol that is likely to be limited to immigration-related screening. More accurately, such vetting includes an evolving form of big data surveillance that attempts to assess criminal and terroristic risk across entire populations and subpopulations through mass data collection, database screening and data fusion, artificial intelligence, and algorithm-driven predictive analytics.[51]

---

46. John Burnett, *Former Immigration Director Defends U.S. Record on Refugee Vetting*, NPR (Feb. 3, 2017, 4:35 PM), http://www.npr.org/2017/02/03/513311323/former-immigration-director-defends-u-s-record-on-refugee-vetting [https://perma.cc/U99Q-RWT5] (noting that the former director of the Office of U.S. Citizenship and Immigration Services of the U.S. Department of Homeland Security under the Obama administration "point[ed] out that his office had been checking Facebook, Twitter and Instagram accounts of prospective refugees from Syria and Iraq since 2015").

47. Alexander Smith, *U.S. Visitors May Have to Hand over Social Media Passwords: DHS*, NBC NEWS (Feb. 8, 2017, 7:51 AM), http://www.nbcnews.com/news/us-news/us-visitors-may-have-hand-over-social-media-passwords-kelly-n718216 [https://perma.cc/7WK4-FDKB].

48. *See id.*; *see also* Notice of Modified Privacy Act System of Records, 82 Fed. Reg. 179 (Sept. 18, 2017).

49. *See, e.g.*, DEP'T OF HOMELAND SEC., *supra* note 33; *see also infra* Part I.A.

50. DHS offers this definition of identity management:

> Identity Management (IdM) deals with identifying and managing individuals within a government, state, local, public, or private sector network or enterprise. In addition, authentication and authorization to access resources such as facilities or, sensitive data within that system are managed by associating user rights, entitlements, and privileges with the established identity.

*Cyber Security Division Identity Management Program Video*, DEP'T HOMELAND SECURITY, https://www.dhs.gov/science-and-technology/cyber-security-division-identity-management-program-video [https://perma.cc/9NGG-8G28] (last visited Oct. 16, 2016).

51. *See, e.g.*, STEVEN FINLAY, PREDICTIVE ANALYTICS, DATA MINING AND BIG DATA: MYTHS, MISCONCEPTIONS AND METHODS 3 (2014); ERIC SIEGEL, PREDICTIVE ANALYTICS: THE POWER TO PREDICT WHO WILL CLICK, BUY, LIE, OR DIE 59–60 (2013); NATE SILVER, THE SIGNAL AND THE NOISE: WHY SO MANY PREDICTIONS FAIL—BUT SOME DON'T 417–18 (2012); *see also* Spencer Woodman, *Palantir Provides the Engine for Donald Trump's Deportation Machine*, INTERCEPT (Mar. 2, 2017, 1:18 PM), https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/ [https://perma.cc/4B2H-JLHV] (reporting that the DHS awarded a private contractor a $41 million contract to build an "Investigative Case Management" system to allow DHS to "access a vast 'ecosystem' of data

The long-term consequences of modern big data surveillance can be better envisioned by anticipating how and why big data vetting protocols may be extended to the entire population. Eventually, all residents of the United States, both citizens and noncitizens, may face various stages of technological vetting and algorithmic screening as a part of a post-September 11, 2001, national security policy trajectory that embraces big data surveillance for its presumed efficacy. Importantly, in parallel with the extreme vetting protocols mandated by the Executive Orders, almost every immigration reform effort since 9/11 has called for biometric data collection from the entire citizenry in the United States to enhance border security efforts.[52] At the same time, increasing concern regarding homegrown terrorism has resulted in a call to extend domestic surveillance and counterterrorism efforts to both citizens and noncitizens.[53] The Snowden disclosures, for example, have further revealed how foreign-intelligence-gathering tools, such as bulk metadata collection, can be indiscriminate in scope and impact both citizens and noncitizens.[54]

Identifying the vetting procedures embedded within Executive Order 13,769 and the constitutional challenges which followed its promulgation is particularly appropriate as 2017 marks the seventy-fifth anniversary of the signing of Executive Order 9066 by President Franklin Delano Roosevelt.[55] That order, issued on February 19, 1942, and titled "Authorizing the Secretary of War to Prescribe Military Areas," allowed for Japanese internment by delegating to the Secretary of War the authority "to take such other steps as he . . . may deem advisable to enforce compliance" with the exclusion of Japanese Americans and those of Japanese ancestry.[56]

The legal challenges mounted against Executive Order 9066 culminated in several U.S. Supreme Court cases, most notably, *Korematsu v. United States*.[57] In this case, decided in 1944, the Court upheld the constitutionality

---

to facilitate immigration officials in both discovering targets and then creating and administering cases against them").

52. *See* Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1478–82 (2013).

53. *See, e.g.*, *Countering Violent Extremism*, DEP'T HOMELAND SECURITY (Jan. 19, 2017), https://www.dhs.gov/countering-violent-extremism [https://perma.cc/5CS6-TL7X]; *see also* TREVOR AARONSON, THE TERROR FACTORY: INSIDE THE FBI'S MANUFACTURED WAR ON TERRORISM 19 (2013); Colin Moynihan, *A New York City Settlement on the Surveillance of Muslims*, NEW YORKER (Jan. 7, 2016), http://www.newyorker.com/news/news-desk/a-new-york-city-settlement-on-surveillance-of-muslims [https://perma.cc/X6J9-Y2EQ] ("After the attacks of September 11, 2001, the New York Police Department began an intense surveillance operation that focused on Muslims in New York City . . . . They eavesdropped on conversations in restaurants and cafes, catalogued memberships in mosques and student organizations, and . . . tried to bait people into making inflammatory statements.").

54. *See, e.g.*, Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 863–64 (2014); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 151–52, 157, 164 n.83, 202–19 (2015).

55. Exec. Order No. 9066, 3 C.F.R. §§ 1092–93 (1942).

56. *Id.*

57. 323 U.S. 214 (1944); *see also* Hirabayashi v. United States, 320 U.S. 81, 100 (1943) ("Distinctions between citizens solely because of their ancestry are by their very nature odious to a free people whose institutions are founded upon the doctrine of equality.").

of Executive Order 9066, reasoning in part: "[W]e are dealing specifically with nothing but an exclusion order. To cast this case into outlines of racial prejudice, without reference to the real military dangers which were presented, merely confuses the issue."[58] Drawing comparisons between Executive Order 13,769 and Executive Order 9066, and reviewing the original justification for Japanese internment, is critical here as President Trump and others have cited both FDR's actions[59] and *Korematsu* as precedent for the Muslim Ban and the development of a Muslim registry database.[60]

This Article proceeds in four parts. Part I describes how modern vetting procedures are intertwined with burgeoning identity-management systems. Based on a review of publicly available information, these vetting protocols are increasingly dependent upon the following: mass biometric data collection, automated or semiautomated biometric identification, and algorithm-dependent database screening programs. In a big data world, threat risk assessments and data-profiling tools do not necessarily begin with the identification of individuals on the basis of traditionally protected classifications, such as race, ethnicity, or national origin. Instead, because contemporary big data systems are data-classification oriented, vetting and screening protocols begin with the identification of individuals on the basis of numerical identification, such as passport numbers, and on the basis of biometric identification, such as the cataloguing of scanned fingerprints and irises.

Part II describes how national security programs risk creating forms of discrimination similar to Jim Crow in that they are also based upon classification and screening protocols. Historic Jim Crow regimes started with a legal premise: that certain individuals could and should be classified on the basis of race. Next, Jim Crow laws utilized screening systems to enforce segregation based upon designated racial classification. This discussion explores why security threat assessments produced through algorithms and database screening may—similar to historic Jim Crow—also separate populations based upon particular classifications. New Algorithmic Jim Crow systems, like historic Jim Crow regimes, systems may present themselves as facially neutral.

---

58. *Korematsu*, 323 U.S. at 223.

59. "What I'm doing is no different than FDR," Trump told ABC News during the presidential campaign. Meghan Keneally, *Donald Trump Cites These FDR Policies to Defend Muslim Ban*, ABC NEWS (Dec. 8, 2015, 1:01 PM), http://abcnews.go.com/Politics/donald-trump-cites-fdr-policies-defend-muslim-ban/story?id=35648128 [https://perma.cc/FY3H-9NNE].

60. Shortly after President Trump's election, Carl Higbie, a former spokesman for the Great America Political Action Committee, stated on Fox News that a Muslim database registry would be legal and would "hold constitutional muster" under *Korematsu*, explaining, "We did it during World War II with the Japanese . . . ." Derek Hawkins, *Japanese American Internment Is 'Precedent' for National Muslim Registry, Prominent Trump Backer Says*, WASH. POST (Nov. 17, 2016), https://www.washingtonpost.com/news/morning-mix/wp/2016/11/17/japanese-internment-is-precedent-for-national-muslim-registry-prominent-trump-backer-says/ [https://perma.cc/SF5A-4HEK].

Part III explains how identity-management systems do not necessarily discriminate based on protected categories recognized under equal protection jurisprudence.[61] Rather, newly emerging vetting systems are often centered on big data and generally driven by mass data collection and analysis. These systems, for instance, purport to be race neutral and not to target individuals based on a protected classification. Rather, it is often the case that results of data screening and vetting analytics deemed suspect and anomalous are isolated and targeted. Consequently, the "equal but separate" consequences of Algorithmic Jim Crow will allow for the "equal" vetting and screening of all citizens and noncitizens. At the same time, newly deployed vetting systems will allow federal and state governments to "separate" individuals based upon the vetting and screening actions mandated through security policy developments.

Part IV further discusses why advocates of immigration federalism[62] and national security federalism[63]—those seeking the expansion of state participation in the enforcement of federal immigration and national security law—have increasingly enacted biometric data harvesting and identity-management laws that mimic federal laws and programs. These state laws mandate the utilization of multiple dataveillance tools and biometric data screening devices, purportedly to further crime and immigration control and simultaneously support counterterrorism efforts. Yet, just as historic Jim Crow regimes delegated segregationist gatekeeping duties to state and private entities, contemporary immigration policy delegates restrictive immigration gatekeeping duties to state and private entities. Under Algorithmic Jim

61. Equal protection jurisprudence and the foundations for differing standards of judicial review based upon protected classification has yielded rich scholarship. *See generally* JOHN HART ELY, DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW 105–81 (1980); Bruce A. Ackerman, *Beyond* Carolene Products, 98 HARV. L. REV. 713, 714–16 (1985); Mario L. Barnes et al., *A Post-Race Equal Protection?*, 98 GEO. L.J. 967 (2010); Katharine T. Bartlett, *Tradition as Past and Present in Substantive Due Process Analysis*, 62 DUKE L.J. 535, 540–48 (2012); Robert M. Cover, *The Origins of Judicial Activism in the Protection of Minorities*, 91 YALE L.J. 1287, 1294–97 (1982); Trina Jones, *Shades of Brown: The Law of Skin Color*, 49 DUKE L.J. 1487 (2000); Michael Klarman, *An Interpretive History of Modern Equal Protection*, 90 MICH. L. REV. 213, 219 (1991); Melissa Murray, *Equal Rites and Equal Rights*, 96 CALIF. L. REV. 1395 (2008); Bertrall L. Ross II, *The Representative Equality Principle: Disaggregating the Equal Protection Intent Standard*, 81 FORDHAM L. REV. 175 (2012); Jed Rubenfeld, *The Anti-Antidiscrimination Agenda*, 111 YALE L.J. 1141, 1143 (2002); Kenji Yoshino, *The New Equal Protection*, 124 HARV. L. REV. 747, 748, 755–63 (2011).

62. Hiroshi Motomura is credited with introducing the term "immigration federalism" into academic discourse to describe state and local involvement in immigration. Peter J. Spiro, *Learning to Live with Immigration Federalism*, 29 CONN. L. REV. 1627, 1627 (1997); *see also* Pratheepan Gulasekaram & S. Karthick Ramakrishnan, *Immigration Federalism: A Reappraisal*, 88 N.Y.U. L. REV. 2074, 2096 (2013); Clare Huntington, *The Constitutional Dimension of Immigration Federalism*, 61 VAND. L. REV. 787, 788 n.6 (2008) (crediting Motomura with "defining immigration federalism as 'states and localities play[ing a role] in making and implementing law and policy relating to immigration and immigrants'" (citing Hiroshi Motomura, *Federalism, International Human Rights, and Immigration Exceptionalism*, 70 U. COLO. L. REV. 1361, 1361 (1999))).

63. *See, e.g.*, Matthew C. Waxman, *National Security Federalism in the Age of Terror*, 64 STAN. L. REV. 289, 289 (2012); *see also* Kris W. Kobach, *Reinforcing the Rule of Law: What States Can and Should Do to Reduce Illegal Immigration*, 22 GEO. IMMIGR. L.J. 459, 475 (2008).

Crow, these technologically enabled gatekeeping duties involve race-neutral database screening of personally identifiable data and biometric data through federal vetting and screening protocols. The results, however, may not be race neutral, or may in fact have a disparate impact on traditionally protected classes.

Part IV further explains how technological vetting protocols and algorithm-driven database screening systems may be insulated from successful legal challenges, as the law has not yet adapted to anticipate new forms of back-end discrimination facilitated by DHS's rapid deployment of identity-management programs. The government, as in *Korematsu*, will likely defend any disparate-impact consequences as necessary and justified based upon threat risk assessments and nonracial classifications. Risk-based classifications and data characteristics deemed suspect fall outside of the protections recognized by current equal protection jurisprudence. This type of disparate impact, driven by database screening and technologically enhanced discrimination, may face limited or lenient review by a federal judiciary that generally grants broad deference to the government in matters of immigration and national security.[64] Thus, the advent of Algorithmic Jim Crow will require an evolution of equality law.

This Article concludes that current algorithm-driven vetting and biometric-biographic identification screening, especially once deployed across the entire citizenry, will likely lead to discriminatory profiling and surveillance on the basis of suspicious data as well as classification-based discrimination. These vetting and screening systems are likely to result in both direct and disparate discrimination, particularly based on race, color, ethnicity, national origin, and religion. In addition, recent immigration-control policy and programs demonstrate the government's interest in delegating immigration-vetting duties to private actors, such as employers, and nonfederal actors, such as state and local law enforcement, which can exacerbate issues of racial profiling and discrimination.

## I. BIRTH OF ALGORITHMIC JIM CROW

When President Trump signed Executive Order 13,769 on January 27, 2017, then-acting Attorney General Sally Yates was taken by surprise.[65] Yates reviewed the Order as well as a number of briefs by individuals who sought to enjoin the Order in federal court and believed that it raised constitutional problems—namely Establishment Clause and due process concerns.[66] Yates later explained to the *New Yorker* that, after reviewing

64. *See, e.g.*, Shirin Sinnar, *Rule of Law Tropes in National Security*, 129 HARV. L. REV. 1566, 1569 (2016); *see also* Sahar F. Aziz, *Policing Terrorists in the Community*, 5 HARV. NAT'L SECURITY J. 147, 222 (2014) (discussing counterterrism law enforcement).

65. *See* Ryan Lizza, *Why Sally Yates Stood Up to Trump*, NEW YORKER (May 29, 2017), http://www.newyorker.com/magazine/2017/05/29/why-sally-yates-stood-up-to-trump [https://perma.cc/JHF9-73DM] (explaining that Yates learned of the Order upon being notified by a deputy who read the news online).

66. *Id.* ("Yates read through the briefs, and thought that two arguments against the order were particularly strong. . . . [The order] arguably violated the Establishment Clause of the First Amendment. And . . . there seemed to be serious due-process questions.").

arguments for and against the first Order, she thought that her two choices were either to resign or to refuse to defend the Order.[67] After reviewing the evidence, Yates believed that the Order was ultimately based on religion and said, "I thought back to Jim Crow laws, or literacy tests. Those didn't say that the purpose was to prevent African-Americans from voting. But that's what the purpose was."[68] Yates drafted a letter to her colleagues at the U.S. Department of Justice, in which she stated: "At present, I am not convinced that the defense of the Executive Order is consistent with these responsibilities nor am I convinced that the Executive Order is lawful."[69] Yates directed Department of Justice attorneys not to defend the Order until she determined that it was appropriate to act.[70] A few hours later, Yates received a letter from the White House that informed her that she had been fired.[71]

Yates's invocation of Jim Crow deserves notice. The former acting Attorney General concluded that the Executive Order might lead to a disparate impact on the basis of protected classifications such as national origin and religion. At the same time, she also recognized that the Executive Order presented itself as facially neutral, much like the facially neutral literacy tests promulgated under Jim Crow laws that disproportionately burdened the voting rights of minority communities.

Under historic Jim Crow, literacy tests, poll taxes, and other obstacles to voting rights were equally applied to all voters.[72] Although these obstacles did not explicitly inquire into voters' race, they nonetheless significantly disenfranchised minority communities. Therefore, they served discriminatory ends even though the race of the voter was never technically a basis for denying access to the ballot.[73]

Much like literacy tests and poll taxes, post-9/11 security initiatives may disproportionately impact minority communities even though they do not explicitly effectuate decisions based on protected attributes. An inquiry into modern-day screening and vetting systems depends upon in an understanding of myriad post-9/11 national security programs and policy initiatives. Contemporary screening and vetting systems utilize algorithms to determine a wide range of questions, including identity and associational assessments, to gauge risk. For example, extreme vetting systems like the one promulgated by the Executive Orders may bring about disproportionate

67. *Id.*

68. *Id.*

69. Letter from Sally Yates, Acting Attorney Gen., Dep't of Justice, to Dep't of Justice (Jan. 30, 2017), https://www.nytimes.com/interactive/2017/01/30/us/document-Letter-From-Sally-Yates.html [https://perma.cc/T7KF-HNUC].

70. *Id.*

71. Lizza, *supra* note 65 ("The statement was sent to thousands of department employees around the country. About four hours later, at around 9 P.M., McGahn's office asked the senior Trump appointee to deliver a letter to Yates, notifying her that she had been fired.").

72. *See, e.g.*, Guy-Uriel E. Charles & Luis Fuentes-Rohwer, *State's Rights, Last Rites, and Voting Rights*, 47 CONN. L. REV. 481, 486 nn.23–24 (2014); Atiba R.Ellis, *The Cost of the Vote: Poll Taxes, Voter Identification Laws, and the Price of Democracy*, 86 DENV. U. L. REV. 1023, 1024 n.7 (2009).

73. Ellis, *supra* note 72, at 1040 n.79, 1041–50.

burdens on minority communities. Potential discrimination facilitated or exacerbated by technological means appearing to be facially neutral may evade legal challenge requiring careful inquiry.

Because big data screening and tracking systems unfold in ways that are difficult to see—for example, through algorithm-driven determinations, internet-based database screening programs, and social media monitoring—it is critical to explore how modern vetting protocols may be linked to preexisting post-9/11 identity-management systems that are dependent upon cybersurveillance and dataveillance tools. To grasp how extreme vetting can be extended to the entire citizenry, it is helpful to compare No Fly database screening systems with potential extreme vetting database screening systems. For example, based on what is known of both programs, it appears that many of the database screening protocols overlap.[74] Part I, therefore, explains how vetting systems will increasingly rely upon database screening, including universal biometric databases, to sweep entire populations and subsets within populations to assess terroristic and criminal risk.

To better understand the Trump administration's policy on extreme vetting, it is important to reconstruct the justification for such a policy based upon historical background and prior policy developments implemented during the Obama administration. Many of the policies advanced by the Executive Order are not only an outgrowth of 9/11, but they are specifically reactive to the Paris attacks in November 2015 and the San Bernardino attack in December 2015. Both terrorist events led to multiple immigration policy proposals and adjustments to current vetting procedures.

On the evening of November 13, 2015, coordinated terrorist attacks were staged in Paris, France, which included mass shootings, suicide bombings, and hostage takings.[75] According to news reports, the terrorist attacks left 129 dead and 352 wounded, including ninety-nine in serious condition.[76] The terrorist group Islamic State in Iraq and Syria (ISIS) immediately claimed responsibility.[77]

According to news accounts, ISIS announced immediately after the Paris attacks that three teams of eight terrorists had carried them out.[78] Seven of the terrorists were reportedly killed through self-detonated suicide bombs.[79] In the days following the attacks, intelligence reports indicated that at least

74. *See, e.g.*, Ibrahim v. Dep't of Homeland Sec., 62 F. Supp. 3d 909, 929 (N.D. Cal. 2014) ("By this order, all defendants shall specifically and thoroughly query the databases maintained by them, such as the TSDB, TIDE, CLASS, KSTF, TECS, IBIS, TUSCAN, TACTICS, and the no-fly and selectee lists . . . .").

75. Adam Nossiter et al., *Three Teams of Coordinated Attackers Carried Out Assault on Paris, Officials Say; Hollande Blames ISIS*, N.Y. TIMES (Nov. 14, 2015), https://www.nytimes.com/2015/11/15/world/europe/paris-terrorist-attacks.html [https://perma.cc/KSJ4-RLT5].

76. *Id.*

77. *Id.*

78. *Id.*

79. Steve Almasy et al., *Paris Massacre: At Least 128 Killed in Gunfire and Blasts, French Officials Say*, CNN (Nov. 14, 2015, 9:48 AM), http://www.cnn.com/2015/11/13/world/paris-shooting/ [https://perma.cc/RU5V-Z3TM].

three of the eight terrorists had used falsified passports.[80] A passport found on the body of a terrorist who had died at the Stade de France ("National Stadium") was reported to be an illegitimate Syrian passport and it was reported that the terrorist had allegedly claimed Syrian refugee status in France.[81] Two other terrorists killed at the National Stadium allegedly carried false Turkish passports.[82] By November 19, 2015, just six days after the attacks, the governors of thirty-one states had announced their refusal to admit or resettle Syrian refugees in their respective states.[83]

One week after the Paris attacks, Michael Ignatieff, formerly the Edward R. Murrow professor of public policy at the Harvard Kennedy School and currently the rector and president of Central European University in Budapest, expressed a position widely held by many experts: an international biometric identification system would help to address the refugee crisis in Europe and simultaneously serve national security interests.[84] He stated that "[t]he world badly needs a new migratory regime—based around an internationally authorized biometric ID card, with a date of permitted entry and a mandatory exit."[85] On November 24, 2015, while standing next to then-President François Hollande of France less than two weeks after the Paris attacks, then-President Barack Obama announced that "the [U.S.] government was developing 'biometric information and other technologies that can make [refugee identification] more accurate.'"[86]

On December 2, 2015, fourteen people were killed and twenty-one were seriously injured in a terrorist attack in San Bernardino, California.[87] The attack consisted of a mass shooting and an attempted bombing.[88] The perpetrators, Syed Rizwan Farook and Tashfeen Malik, a married couple residing in California, targeted a San Bernardino County Department of

80. Christiane Amanpour & Thom Patterson, *Passport Linked to Terrorist Complicates Syrian Refugee Crisis*, CNN (Nov. 15, 2015, 12:24 PM), http://www.cnn.com/2015/11/15/europe/paris-attacks-passports/index.html [https://perma.cc/HLB4-SJUX].

81. *Id.*

82. *Id.*

83. Ashley Fantz & Ben Brumfield, *More Than Half the Nation's Governors Say Syrian Refugees Not Welcome*, CNN (Nov. 19, 2015, 3:20 PM), http://www.cnn.com/2015/11/16/world/paris-attacks-syrian-refugees-backlash/ [https://perma.cc/VW6W-8FFF] (reporting that the many states refused to accept Syrian refugees for resettlement, including: Alabama, Arizona, Arkansas, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Wisconsin, and Wyoming).

84. *See* Michael Ignatieff, *The Refugees and the New War*, N.Y. REV. BOOKS (Dec. 17, 2015), http://www.nybooks.com/articles/2015/12/17/refugees-and-new-war/ [https://perma.cc/5A9J-5L3V].

85. *Id.*; *see also* Katie Worth, *Can Biometrics Solve the Refugee Debate?*, PBS (Dec. 2, 2015), http://www.pbs.org/wgbh/frontline/article/can-biometrics-solve-the-refugee-debate/ [https://perma.cc/XT36-TMK6].

86. Markowitz, *supra* note 44.

87. Michael S. Schmidt & Richard Pérez-Peña, *F.B.I. Treating San Bernardino Attack as Terrorism Case*, N.Y. TIMES (Dec. 4, 2015), https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html [https://perma.cc/MRP4-KFPJ].

88. *Id.*

Public Health holiday party.[89] Farook, a Pakistani American U.S. citizen born in Illinois, was employed by the Department of Public Health.[90] Malik was a Pakistani-born lawful permanent resident who had recently migrated to the United States.[91] According to media accounts, the Muslim couple had been self-radicalized, inspired by ISIS.[92]

On the same day as the San Bernardino attack, Paul Ryan, Speaker of the U.S. House of Representatives, explained that lawmakers were considering various legislative reforms to increase security vetting of refugees and immigrants in response to the threat of ISIS, including requiring countries "to issue smart e-passports with biometric chips."[93]

Less than one week later, in the immediate aftermath of the Paris and San Bernardino attacks, then-presidential candidate Trump called for what has been referred to as a "Muslim Ban" or "Travel Ban": an executive action that would prohibit entry of any Muslim into the United States.[94] Trump did not provide specifics on how he would prohibit Muslims from entering the United States; however, he later clarified that the ban would be temporary to allow the government to assess its current immigration procedures and "suspend immigration from regions linked with terrorism."[95] Trump's call for a "Muslim Ban" was followed by calls for surveillance of Muslim communities and mosques.[96]

Six months later, on June 12, 2016, Omar Mateen, an Afghani American born in the United States, killed forty-nine people and wounded fifty-three in a shooting rampage at the Pulse nightclub in Orlando, Florida.[97] According to news reports, Mateen had proclaimed allegiance to ISIS shortly before committing "the worst mass shooting in United States history."[98] In the wake of the Orlando attack, then-candidate Trump explained that the profiling of Muslims in the United States was necessary as a preemptive measure to prevent future attacks.[99]

---

89. *Id.*
90. *Id.*
91. *Id.*
92. *Id.*
93. Lisa Lambert et al., *House to Consider Changes to Visa Waiver Program, Including 'Smart' Passports*, REUTERS (Dec. 2, 2015, 8:16 AM), http://www.reuters.com/article/2015/12/02/us-usa-congress-visas-idUSKBN0TL1CV20151202 [https://perma.cc/W32F-SLZR].
94. *See* Diamond, *supra* note 1.
95. Associated Press, *How Donald Trump's Plan to Ban Muslims Has Evolved*, FORTUNE (June 28, 2016), http://fortune.com/2016/06/28/donald-trump-muslim-ban/ [https://perma.cc/X29Y-XCPM].
96. *See* David Mark & Jeremy Diamond, *Trump: 'I Want Surveillance of Certain Mosques,'* CNN (Nov. 21, 2015), http://www.cnn.com/2015/11/21/politics/trump-muslims-surveillance/ [https://perma.cc/78YW-SQEV].
97. *See* Lizette Alvarez et al., *Orlando Gunman Was 'Cool and Calm' After Massacre, Police Say*, N.Y. TIMES (June 13, 2016), https://www.nytimes.com/2016/06/14/us/orlando-shooting.html [https://perma.cc/8VX9-98WB].
98. Lizette Alvarez & Richard Pérez-Peña, *Orlando Gunman Attacks Gay Nightclub, Leaving 50 Dead*, N.Y. TIMES (June 12, 2016), https://www.nytimes.com/2016/06/13/us/orlando-nightclub-shooting.html [https://perma.cc/BP5N-6MHX].
99. *See* Emily Schultheis, *Donald Trump: U.S. Must "Start Thinking About" Racial Profiling*, CBS NEWS (June 19, 2016), http://www.cbsnews.com/news/donald-trump-after-orlando-racial-profiling-not-the-worst-thing-to-do/ [https://perma.cc/8XG8-7E23].

On August 16, 2016, Trump announced a proposal for the "extreme vetting" of immigrants and refugees in a campaign speech on ISIS.[100] He explained: "In the Cold War, we had an ideological screening test. The time is long overdue to develop a new screening test for the threats we face today. I call it extreme vetting. I call it extreme, extreme vetting."[101] Then, on August 31, 2016, Trump delivered an address on his proposed immigration policy.[102] In addition to his promise to build a wall on the southern border of the United States and his reassertion that "Mexico will pay for the wall," Trump explained that he would also implement a "biometric entry-exit system for tracking visa-holders."[103] These promises of enhanced national security and border security systems, as well as the various Executive Orders restricting travel, inherently represent technological developments in the promulgation of emerging cybersurveillance technologies and algorithmic-driven screening and vetting protocols. To draw parallels between historic Jim Crow and Algorithmic Jim Crow, this Article turns to an overview of Jim Crow.

## II. OVERVIEW OF JIM CROW: CLASSIFICATION AND SCREENING SYSTEMS

Artificial intelligence and algorithms are not usually perceived as resulting in discrimination. In fact, they may appear to be equality-compliant or even equality-enhancing in that algorithmic screening and vetting can be applied equally across entire populations and subpopulations. Screening and classification systems, however, even when facially neutral and algorithmically based, can lead to profound constitutional challenges. The historical framing in this section is necessary to assist in the interrogation of new classification and screening systems that are flourishing under security rationales and presented as technologically objective and colorblind.

Therefore, to better grasp why the framing of Algorithmic Jim Crow is now needed, Part II lays a factual predicate to explain the foundational legal premises for historic Jim Crow regimes. Traditional Jim Crow laws first required the government—often state and county governments—to engage in formal and standardized protocols to assign racial classification to citizens of that state or county. Once a racial classification system was determined under the law, screening protocols, also established under Jim Crow laws, enabled the separation of populations on the basis of that racial classification. Consequently, understanding the basic mechanics of how separation was enforced under the law begins with an understanding of historic Jim Crow classification and screening systems.

100. *See, e.g.*, Diamond, *supra* note 1.
101. Diamond, *supra* note 22.
102. Emily Schultheis, *Donald Trump Doubles Down in Immigration Speech: "Mexico Will Pay for the Wall,"* CBS NEWS (Aug. 31, 2016), http://www.cbsnews.com/news/donald-trump-delivers-immigration-speech-in-phoenix/ [https://perma.cc/E59J-RR2S].
103. *Id.*

### *A. Historical Framing of Jim Crow*

This overview is not intended to be an exhaustive history of the legal issues and the nature of Jim Crow—other scholarship has addressed that subject in thoughtful detail.[104] Instead, this background intends to sketch out an understanding of the scope and context of the Jim Crow era and to further clarify that its laws and policies were not confined merely to segregating locational sites and imposing restrictions on movement. Rather, Jim Crow was:

> [A] structure of exclusion and discrimination devised by white Americans to be employed principally against black Americans . . . . Its central purpose was to maintain a second-class social and economic status for blacks while upholding a first-class social and economic status for whites. . . . In the South, Jim Crow discrimination at its height existed not only by statute but by custom and racial 'etiquette,' and it was rigidly enforced by both the law enforcement agencies and courts as well as by ordinary white citizens who were neither policemen nor judges but who often took the law into their own hands as though they were.[105]

---

104. *See generally* 1 RACE, LAW, AND AMERICAN HISTORY 1700–1990: AFRICAN AMERICANS AND THE LAW (Paul Finkelman ed., 1992); FRANK J. SCATURRO, THE SUPREME COURT'S RETREAT FROM RECONSTRUCTION: A DISTORTION OF CONSTITUTIONAL JURISPRUDENCE (2000); STEPHEN L. WASBY ET AL., DESEGREGATION FROM *BROWN* TO *ALEXANDER* (1977); C. VANN WOODWARD, THE STRANGE CAREER OF JIM CROW (3d rev. ed. 2002); Gabriel J. Chin, *Jim Crow's Long Goodbye*, 21 CONST. COMMENT. 107 (2004); Gabriel J. Chin & Randy Wagner, *The Tyranny of the Minority: Jim Crow and the Counter-Majoritarian Difficulty*, 43 HARV. C.R.-C.L.L. REV. 65 (2008); James W. Fox, Jr., *Doctrinal Myths and the Management of Cognitive Dissonance: Race, Law, and the Supreme Court's Doctrinal Support of Jim Crow*, 34 STETSON L. REV. 293 (2005); James W. Fox, Jr., *Intimations of Citizenship: Repressions and Expressions of Equal Citizenship in the Era of Jim Crow*, 50 HOW. L.J. 113 (2006); Rachel D. Godsil, *Race Nuisance: The Politics of Law in the Jim Crow Era*, 105 MICH. L. REV. 505 (2006); Ariela J. Gross, *Litigating Whiteness: Trials of Racial Determination in the Nineteenth-Century South*, 108 YALE L.J. 109 (1998); Trina Jones, Brown II*: A Case of Missed Opportunity?*, 24 L. & INEQ. 9 (2006); José Roberto Juárez, Jr., *Recovering Texas History: Tejanos, Jim Crow, Lynchings & the University of Texas School of Law*, 52 S. TEX. L. REV. 85 (2010); Kenneth W. Mack, *Foreword: A Short Biography of the Civil Rights Act of 1964*, 67 SMU L. REV. 229 (2014); Kenneth W. Mack, *Law, Society, Identity, and the Making of the Jim Crow South: Travel and Segregation on Tennessee Railroads, 1875–1905*, 24 L. & SOC. INQUIRY 377 (1999) [hereinafter Mack, *Law, Society, Identity*]; Kenneth W. Mack, *Rethinking Civil Rights Lawyering and Politics in the Era Before* Brown, 115 YALE L.J. 256 (2005); David Martin, *The Birth of Jim Crow in Alabama 1865–1896*, 13 NAT'L BLACK L.J. 184 (1993); Jennifer Roback, *Southern Labor Law in the Jim Crow Era: Exploitative or Competitive*, 51 U. CHI. L. REV. 1161 (1984); Benno C. Schmidt, Jr., *Principle and Prejudice: The Supreme Court and Race in the Progressive Era. Part 1: The Heyday of Jim Crow*, 82 COLUM. L. REV. 444 (1982); Barbara Y. Welke, *Beyond* Plessy*: Space, Status, and Race in the Era of Jim Crow*, 2000 UTAH L. REV. 267; John W. Wertheimer et al., *"The Law Recognizes Racial Instinct":* Tucker v. Blease *and the Black-White Paradigm in the Jim Crow South*, 29 L. & HIST. REV. 471 (2011); Joseph R. Palmore, Note, *The Not-So-Strange Career of Interstate Jim Crow: Race, Transportation, and the Dormant Commerce Clause, 1878–1946*, 83 VA. L. REV. 1773 (1997); Anders Walker, *Jim Crow's Unwritten Code*, JOTWELL (Jan. 16, 2017), https://legalhist.jotwell.com/jim-crows-unwritten-code/ [https://perma.cc/K4EH-J6K7].

105. JERROLD M. PACKARD, AMERICAN NIGHTMARE: THE HISTORY OF JIM CROW vii–viii (2002). For other sources on the history and impact of Jim Crow, see generally F. MICHAEL HIGGINBOTHAM, GHOSTS OF JIM CROW: ENDING RACISM IN POST-RACIAL AMERICA (2013);

One scholar explains that Jim Crow is a term for "a series [of] laws and ordinances passed by Southern states and municipalities between 1877 and 1965 legalizing segregation (the physical separation of individuals based on race, gender, religion, or class) within their boundaries."[106] Although racial discrimination was not a solely Southern practice—African Americans in Northern states experienced discrimination in housing, education, employment, and economic settings[107]—in the South, racial restrictions were omnipresent and ingrained in Southern life.[108] One historian argues that Jim Crow "was a Southern phenomenon, the infrastructure white Southerners built to preserve, insofar as humanly possible, the old master/slave system."[109]

Jim Crow penetrated every facet of life for Southern African Americans: it was an integral part of the social, political, and legal fabric of Southern society.[110] Jim Crow established restrictions on marriage,[111] voting,[112]

---

HOLLOWAY, *supra* note 23; KIMBERLEY JOHNSON, REFORMING JIM CROW: SOUTHERN POLITICS AND STATE IN THE AGE BEFORE *BROWN* (2010); STETSON KENNEDY, JIM CROW GUIDE: THE WAY IT WAS (Fl. Atl. Univ. Press 1990) (1959); MICHAEL J. KLARMAN, FROM JIM CROW TO CIVIL RIGHTS: THE SUPREME COURT AND THE STRUGGLE FOR RACIAL EQUALITY (2004); PAULI MURRAY, STATES' LAWS ON RACE AND COLOR (1950); REMEMBERING JIM CROW: AFRICAN AMERICANS TELL ABOUT LIFE IN THE SEGREGATED SOUTH (William H. Chafe et al. eds., 2001); THE FOLLY OF JIM CROW: RETHINKING THE SEGREGATED SOUTH (Stephanie Cole & Natalie J. Ring eds., 2012); LESLIE V. TISCHAUSER, JIM CROW LAWS (2012); WOODWARD, *supra* note 104; RICHARD WORMSER, THE RISE AND FALL OF JIM CROW (2003); Stephen Ansolabehere & Samuel Issacharoff, *The Story of* Baker v. Carr, *in* CONSTITUTIONAL LAW STORIES 271 (Michael C. Dorf ed., 2d ed. 2009); Cheryl I. Harris, *The Story of* Plessy v. Ferguson*: The Death and Resurrection of Racial Formalism*, *in* CONSTITUTIONAL LAW STORIES, *supra* at 187.

106. TISCHAUSER, *supra* note 105, at 1. For an overview of state laws on race during the Jim Crow era, see generally MURRAY, *supra* note 105.

107. PACKARD, *supra* note 105, at 64.

108. *See, e.g.*, MURRAY, *supra* note 105, at 21–34, 38–50, 77–117, 164–95, 198–211, 237–50, 329–48, 406–22, 427–56, 461–90 (detailing state laws on race in effect during the Jim Crow era in Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Maryland, Mississippi, North Carolina, South Carolina, Tennessee, Texas, and Virginia); PACKARD, *supra* note 105, at 62–65; TISCHAUSER, *supra* note 105, at 35–37; *see also* THOMAS PEARCE BAILEY, RACE ORTHODOXY IN THE SOUTH AND OTHER ASPECTS OF THE NEGRO QUESTION 92–93 (1914) (describing "the racial creed of the Southern people").

109. PACKARD, *supra* note 105, at 64.

110. *Id.* at 64–65.

111. *See* KENNEDY, *supra* note 105, at 63–71; TISCHAUSER, *supra* note 105, at 150–51; James R. Browning, *Anti-Miscegenation Laws in the United States*, 1 DUKE B.J. 26, 31 (1951); Paul A. Lombardo, *Miscegenation, Eugenics, and Racism: Historical Footnotes to* Loving v. Virginia, 21 U.C. DAVIS L. REV. 421, 425–26 & n.18 (1988) (discussing judicial decisions supporting antimiscegenation laws); *see also* Loving v. Commonwealth, 147 S.E.2d 78, 83 (Va. 1966) (upholding Virginia's antimiscegenation statute). *But see* Loving v. Virginia, 388 U.S. 1, 12 (1967) ("There can be no doubt that restricting the freedom to marry solely because of racial classifications violates the central meaning of the Equal Protection Clause.").

112. *See, e.g.*, KENNEDY, *supra* note 105, at 147–64; KLARMAN, *supra* note 105, at 28–39; TISCHAUSER, *supra* note 105, at 47–50; Ansolabehere & Issacharoff, *supra* note 105, at 297; *see also* Williams v. Mississippi, 170 U.S. 213, 225 (1898) (concluding that state constitutional requirements of poll taxes and literacy for voting did not discriminate based on race). *But see* Harper v. Va. Bd. of Elections, 383 U.S. 663, 666 (1966) ("We conclude that a State violates the Equal Protection Clause of the Fourteenth Amendment whenever it makes the affluence of the voter or payment of any fee an electoral standard. . . . [T]he Equal Protection Clause of the Fourteenth Amendment restrains the States from fixing voter

education,[113] employment,[114] housing,[115] travel,[116] and enforced segregation in public spaces.[117] Some of these restrictions were codified in law, and others were ingrained as a matter of social behavior and custom.[118] Jim Crow "stood for an entire culture based on violence, racism, and fear that affected the life of every African American living in the South."[119] Despite the passage of the Thirteenth, Fourteenth, and Fifteenth Amendments, Supreme Court precedent in the wake of those amendments upheld laws that enforced racial inequality through segregation laws, or laws that created a disproportionately discriminatory impact on African Americans.[120]

Racial classification was an integral part of Jim Crow.[121] The majority of the Southern states legalized racial classification by codifying the "one-drop" rule or enshrining it as part of their state constitutions: any modicum of black ancestry meant that the individual in question was not white, and thus subject

---

qualifications which invidiously discriminate."); Louisiana v. United States, 380 U.S. 145, 154–56 (1965) (finding that state constitutional provisions that require voters to satisfy voting registrars that they understand and can interpret the U.S. or Louisiana constitutions violate the Constitution and are inconsistent with prohibitions against race-based voting discrimination under the Fifteenth Amendment); United States v. Mississippi, 380 U.S. 128, 151 (1965) (concluding that the attorney general has the power to sue a state and state officials to protect voting rights of African American citizens).

113. *See* KENNEDY, *supra* note 105, at 86–108; TISCHAUSER, *supra* note 105, at 38–46, 116–17 (discussing the impact of Jim Crow policies in education). *But see* Brown v. Bd. of Educ., 347 U.S. 483, 495 (1954) (holding that segregation of public educational facilities results in deprivation of equal protection under the Fourteenth Amendment and that "[s]eparate educational facilities are inherently unequal"); McLaurin v. Okla. State Regents, 339 U.S. 637, 642 (1950); Sweatt v. Painter, 339 U.S. 629, 634–35 (1950).

114. *See* KENNEDY, *supra* note 105, at 109–30.

115. *See* TISCHAUSER, *supra* note 105, at 68–69 ("Some towns excluded all people of color from residing anywhere within their boundaries, or, in the case of 'sundown towns,' had laws making it a crime for people of color to be found within city limits after 8:00 p.m."). *But cf.* Shelley v. Kraemer, 334 U.S. 1, 22 (1948).

116. *See* Plessy v. Ferguson, 163 U.S. 537, 551–52 (1896), *overruled by Brown*, 347 U.S. 483; KENNEDY, *supra* note 105, at 178–89; A. K. Sandoval-Strausz, *Travelers, Strangers, and Jim Crow: Law, Public Accommodations, and Civil Rights in America*, 23 L. & HIST. REV. 53, 54 (2005); *see also* Heart of Atlanta Motel, Inc., v. United States, 379 U.S. 241, 257 (1964).

117. *See, e.g.*, KENNEDY, *supra* note 105, at 190–202; TISCHAUSER, *supra* note 105, at 68 ("By 1920, Southern state legislatures and governors had passed more than 350 segregation laws . . . [that] separated people by race in cemeteries, churches, hospitals, labor unions, prisons, offices, factories, mines, parks, public buildings, railway trains, railway station waiting rooms, housing developments, neighborhoods, schools, stores, streetcars, theaters, funeral parlors, and any other places people could meet."); Harris, *supra* note 105, at 187. *See generally* PACKARD, *supra* note 105.

118. *See, e.g.*, KENNEDY, *supra* note 105, at 203–27 (discussing "[t]he [d]ictates of [r]acist [e]tiquette"). *See generally* REMEMBERING JIM CROW, *supra* note 105.

119. *See* TISCHAUSER, *supra* note 105, at 2.

120. *See, e.g.*, Williams v. Mississippi, 170 U.S. 213, 222–25 (1898); *Plessy*, 163 U.S. at 544; The Civil Rights Cases, 109 U.S. 3, 25–26 (1883).

121. *See* IAN HANEY LÓPEZ, WHITE BY LAW: THE LEGAL CONSTRUCTION OF RACE 81–86 (rev. ed. 2006) (discussing segregation era laws and arguing that law "constructs racial differences on several levels through the promulgation and enforcement of rules that determine permissible behavior"); PACKARD, *supra* note 105, at 94–100 (discussing racial definitions and state laws identifying which citizens were not considered white); Gross, *supra* note 104, at 177–78; Jones, *supra* note 61, at 1487, 1495–96 & nn.25–26; *see also infra* note 122.

to Jim Crow laws.[122] Definitions of race were also included in antimiscegenation laws, which prohibited interracial marriage.[123] Virginia, for example, adopted a law that required racial descriptions to be recorded at a child's birth to further classify individuals as "white" or "colored."[124] Virginia's Racial Integrity Act of 1924[125] "required all citizens within the state born after June 14, 1912 to register their racial composition with the Bureau of Vital Statistics,"[126] prohibited interracial marriages, and defined who exactly qualified as "white."[127] A copy of an old birth record form provided by the Library of Virginia describes the definition of "white" under Virginia law: "A white person is one with no trace whatever of blood of another race, except that one with one-sixteenth of the blood of American Indian, unmixed with other race, may be classed as white."[128]

Thus, the Jim Crow system depended on initial classification and markers of racial identity to determine who would be subjected to laws that designated individual treatment, rights, and privileges based on those classifications.[129]

### *B. Classification and Screening*

Classification of identity, such as the race-based types that occurred during the Jim Crow era, is an essential step in establishing exclusionary systems.[130]

---

122. *See, e.g.*, OKLA. CONST. of 1907, art. XXIII, § 11; ALA. CODE tit. 1, § 2 (1940); ARK. STAT. ANN. § 41-808 (1947); FLA. STAT. ANN. § 1.01 (1941); GA. CODE ANN. §§ 79-103, 53-312 (1935); TENN. CODE. ANN. § 25 (1934); TEX. STAT. ANN. art. 2900 (1947); TEX. PENAL CODE ANN. art. 493, art. 1661, § 2 (1947); VA. CODE ANN. § 1-14 (1950); Asher v. Huffman, 174 S.W.2d 424, 425 (Ky. 1943) (interpreting the Kentucky Constitution to define white and colored children); Lee v. New Orleans Great N. R.R., 51 So. 182, 183 (La. 1910) (defining "colored persons"); Moreau v. Grandich, 75 So. 434, 435 (Miss. 1917) (construing provisions of the Mississippi Constitution to define a "colored" person); *see also* LÓPEZ, *supra* note 121, at 83; PACKARD, *supra* note 105, at 98; Jones, *supra* note 61, at 1503–11. *See generally* MURRAY, *supra* note 105 (providing an overview of the antidiscrimination and segregation laws of the fifty states); Christine B. Hickman, *The Devil and the One Drop Rule: Racial Categories, African Americans, and the U.S. Census*, 95 MICH. L. REV. 1161 (1997); Daniel J. Sharfstein, *Crossing the Color Line: Racial Migration and the One-Drop Rule, 1600–1860*, 91 MINN. L. REV. 592 (2007).

123. *See, e.g.*, N.C. CONST. of 1875, art. XIV, § 8 (prohibiting interracial marriage, including a "person of Negro descent to the third generation"); MD. CODE ANN. art. 27, § 445 (1939) (prohibiting interracial marriages as well as marriages to descendants of certain races "to the third generation").

124. *See* An Act to Preserve Racial Integrity, ch. 371, § 5, 1924 Va. Acts 534, 535 (repealed 1975), *invalidated in part by* Loving v. Virginia, 388 U.S. 1 (1967); *see also* Richard B. Sherman, *"The Last Stand": The Fight for Racial Integrity in Virginia in the 1920s*, 54 J. SOUTHERN HIST. 69, 70–71 (1988).

125. An Act to Preserve Racial Integrity § 5.

126. Kevin Noble Maillard, *The Pocahontas Exception: The Exemption of American Indian Ancestry from Racial Purity Law*, 12 MICH. J. RACE & L. 351, 369 (2007).

127. *Id.* at 369–70.

128. *Registration of Birth and Color, 1924*, EDUC. @ LIBR. VA., http://edu.lva.virginia.gov/online_classroom/shaping_the_constitution/doc/birth_registration [https://perma.cc/CSV7-EDX4] (last visited Oct. 16, 2017) (making available Form 59-3-17-24-65M, titled "Registration of Birth and Color–Virginia").

129. *See, e.g.*, PACKARD, *supra* note 105, at 94–100.

130. *See, e.g.*, Kitty Calavita, *The Paradoxes of Race, Class, Identity, and "Passing": Enforcing the Chinese Exclusion Acts, 1882–1910*, 25 L. & SOC. INQUIRY 1, 26 (2000); Andrew M. Carlon, *Racial Adjudication*, 2007 BYU L. REV. 1151, 1169–70; Jones, *supra* note

Exclusion involves separating out individuals from a group or one group from another category. It is not possible to exclude a group from a system of rights and privileges without first determining criteria for exclusion.[131] Therefore, classification is necessary for these systems' operation.[132] During the Jim Crow era, these classifications took the form of "one-drop" laws, or legal decisions that identified who was "colored" and who was not.[133] Other exclusionary systems have engaged in similar forms of classification. For example, Apartheid in South Africa relied on national identity cards that identified individuals by racial groups.[134] During the Belgian colonial period in Rwanda, officials mandated "Hutu" and "Tutsi" markers on identity cards in a system that privileged Tutsi individuals and ultimately laid the groundwork for the 1994 genocide.[135] In Nazi Germany, the Nuremburg laws determined who was Jewish and thus subject to exclusion, discrimination, and persecution.[136]

Classification alone, however, is not sufficient to operate an exclusionary system. Implementing such a system requires screening: determining whether individuals who have been classified are complying with the rules that accompany such classification or whether the individuals are somehow "suspect." Under Jim Crow, for example, screening was both official—such as official segregation policy enforcement—and unofficial, as a part of social

---

61, at 1495–97. David Lyon points out that classification (or categorization) is also an essential part of "[a]ll modern social institutions." David Lyon, *Surveillance as Social Sorting: Computer Codes and Mobile Bodies*, *in* SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK, AND DIGITAL DISCRIMINATION 13, 21 (David Lyon ed., 2003).

131. *See, e.g.*, Akhil Reed Amar, *Becoming Lawyers in the Shadow of* Brown, 40 WASHBURN L.J. 1, 10–11 (2000); Calavita, *supra* note 130, at 10–11, 15–17, 20–23; Christopher A. Ford, *Administering Identity: The Determination of "Race" in Race-Conscious Law*, 82 CALIF. L. REV. 1231, 1274–75 (1994). For a discussion of what constitutes a government racial classification, see generally Stephen Menendian, *What Constitutes a "Racial Classification?": Equal Protection Doctrine Scrutinized*, 24 TEMP. POL. & C.R.L. REV. 81 (2014).

132. *See, e.g.*, Jim Fussell, Prevent Genocide Int'l, Presentation to the Seminar Series of the Yale University Genocide Studies Program (Nov. 15, 2001), http://genocidewatch.org/images/AboutGen_Group_Classification_on_National_ID_Cards.pdf [https://perma.cc/TN5V-TJLC].

133. *See supra* notes 121–28 and accompanying text; *see also* Ford, *supra* note 131, at 1274–75.

134. *See, e.g.*, Keith Breckenridge, *Verwoerd's Bureau of Proof: Total Information in the Making of Apartheid*, 59 HIST. WORKSHOP J. 83, 90 (2005); Carlon, *supra* note 130, at 1170; Ford, *supra* note 131, at 1276–79; Paul N. Edwards & Gabrielle Hecht, *History and the Technopolitics of Identity: The Case of Apartheid South Africa*, 36 J. S. AFR. STUD. 619, 625–28 (2010).

135. *See, e.g.*, PHILIP GOUREVITCH, WE WISH TO INFORM YOU THAT TOMORROW WE WILL BE KILLED WITH OUR FAMILIES: STORIES FROM RWANDA 55–58 (1998); Fussell, *supra* note 132, at 1; Helen M. Hintjens, *When Identity Becomes a Knife: Reflecting on the Genocide in Rwanda*, 1 ETHNICITIES 25, 30–31 (2001).

136. MARION A. KAPLAN, BETWEEN DIGNITY AND DESPAIR: JEWISH LIFE IN NAZI GERMANY 77–79 (1999); David Bankier, *Hitler and the Policy-Making Process on the Jewish Question*, 3 HOLOCAUST & GENOCIDE STUD. 1, 14 (1988); Fussell, *supra* note 132, at 1. Scholarship has linked the Nuremburg laws to Jim Crow laws from the American South. *See* JAMES Q. WHITMAN, HITLER'S AMERICAN MODEL: THE UNITED STATES AND THE MAKING OF NAZI RACE LAW 103–04 (2017).

and behavioral norms.[137] Jim Crow-era screening was a "small data" world screening system, relying first on classification on paper documents, such as birth certificates or identity cards, or an examination of physical appearance,[138] followed by screening to ensure that the excluded individuals complied with the systems of classification.[139] In a big data world, systems of screening, such as the extreme vetting requirements of Trump's Executive Orders, are capable of surveilling vast numbers of individuals based on data or other broad categories and then subsequently classifying them based on status.[140] Essentially, screening is now theoretically "equal" and the classification system is "separate."

Failing to examine the underlying bases of classification and screening systems indicates an inherent level of trust in government systems that ultimately may lead to harmful consequences.[141] Screening in a big data world serves as a form of technological interrogation and entrenches surveillance as a norm.[142] Mass screenings of citizens in "collect it all" systems embed the structure of policing into the state in much the same way that Jim Crow embedded racial classifications and screenings of individuals based on race or perceived race.[143] Big data systems seek suspicious data as a means of identifying and classifying suspicious persons.[144] Broad population-based screening and mass surveillance promote fundamentally undemocratic surveillance norms.[145] As Justice Sotomayor explained in her

137. *See supra* notes 104–20 and accompanying text.

138. *See* Ford, *supra* note 131, at 1275; Jones, *supra* note 61, at 1496 n.26; *supra* notes 121–24 and accompanying text.

139. Ford, *supra* note 131, at 1275–76; Harris, *supra* note 105, at 187–90; Jones, *supra* note 61, at 1496 n.26.

140. *See supra* Part I.A; *see also* Lyon, *supra* note 130, at 13 ("Abstract data, now including video, biometric, and genetic as well as computerized administrative files, are manipulated to produce profiles and risk categories in a liquid, networked system. The point is to plan, predict, and prevent by classifying and assessing those profiles and risks.").

141. *See, e.g.*, David Lyon, James B. Rule & Etienne Combet, *Identity Cards: Social Sorting by Database*, OXFORD INTERNET INST. INTERNET ISSUE, Nov. 2004, at 2; Daniel J. Steinbock, *National Identity Cards: Fourth and Fifth Amendment Issues*, 56 FLA. L. REV. 697, 699 (2004).

142. Lyon, *supra* note 130, at 21 ("The individualization of risk thus fosters ever-spiraling levels of surveillance, implying that automated categorization occurs with increasing frequency.").

143. *See supra* notes 121–28 and accompanying text.

144. *See, e.g.*, Margaret Hu, *From the National Surveillance State to the Cybersurveillance State*, 13 ANN. REV. L. & SOC. SCI. (forthcoming 2017); Jeremy Scahill & Glenn Greenwald, *The NSA's Secret Role in the U.S. Assassination Program*, INTERCEPT (Feb. 10, 2014, 12:03 AM), https://theintercept.com/2014/02/10/the-nsas-secret-role/ [https://perma.cc/Z32Z-4TZ6].

145. *See, e.g.*, Utah v. Strieff, 136 S. Ct. 2056, 2070–71 (2016) (Sotomayor, J., dissenting); Florida v. Riley, 488 U.S. 445, 456–67 (1989) (Brennan, J., dissenting); United States v. White, 401 U.S. 745, 792–93 (1971) (White, J., dissenting); Boyd v. United States, 116 U.S. 616, 630 (1886); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 17–18 (2008); Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489, 490 (2006); Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1775–76 (2014);

dissenting opinion in *Utah v. Strieff*,[146] random, suspicionless identity verifications by law enforcement on the street are inherently undemocratic:

> [T]his case tells everyone, white and black, guilty and innocent, that an officer can verify your legal status at any time. It says that your body is subject to invasion while courts excuse the violation of your rights. It implies that you are not a citizen of a democracy, but the subject of a carceral state, just waiting to be cataloged.[147]

Further, some screening protocols may rely on rationales that are facially neutral but ultimately based on impermissible classifications. In his concurring opinion in *International Refugee Assistance Project v. Trump*,[148] Judge James Wynn pointed out that discrimination, even when "shrouded in layers of legality[,] is no less an insult to our Constitution than naked invidious discrimination."[149] Judge Wynn cited *Dred Scott v. Sandford*[150] and *Korematsu v. United States*[151] as examples of judicial failures in response to exclusionary and discriminatory systems cloaked in legality.[152] In the majority opinion, the Fourth Circuit concluded that the plaintiffs had sufficiently alleged that nationality served as a proxy for religious discrimination[153] and was a crude and ineffective measure for determining whether a threat existed.[154] Indeed, in her decision to refuse to defend the first Executive Order, then-acting Attorney General Sally Yates considered that it bore a resemblance to Jim Crow laws.[155]

Thus, systems of subordination, such as Jim Crow and Apartheid, depend on classifying who is privileged and who is not. As discussed above, once a classification is emplaced, laws can require separation, subordination, and screening on the basis of that classification. Jim Crow regimes used race-based classifications to engage in a broad range of economic, social, and political exclusions under the law.[156] The act of excluding or disenfranchising on the basis of race often required legally mandated

---

Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 251 (2002).

146. 136 S. Ct. 2056 (2016).

147. *Id.* at 2070–71 (Sotomayor, J., dissenting). *Strieff* addressed whether the discovery of a valid arrest warrant was sufficiently attenuating such that evidence discovered during an initially unconstitutional investigatory stop was admissible. *Id.* at 2059 (majority opinion).

148. 857 F.3d 554 (4th Cir.), *cert. granted*, 137 S. Ct. 2080 (2017).

149. *Id.* at 612 (Wynn, J., concurring).

150. 60 U.S. 393 (1857).

151. 323 U.S. 214 (1944).

152. *Int'l Refugee Assistance Project*, 857 F.3d at 612 (Wynn, J., concurring).

153. *See id.* at 591–92 (majority opinion) (discussing the evidence that "national security is not the true reason for EO-2," including statements made by Trump as a candidate, statements made by his advisors after he assumed office, and the issuance of both the first and second Executive Orders); *see also id.* at 613 (Wynn, J., concurring) ("[T]he Executive Order here relies on national origin as a proxy for discrimination based on religious animus . . . .").

154. *See id.* at 596 (majority opinion) (citing internal reports from the Department of Homeland Security and an amicus brief from former national security officials that concluded that nationality-based screening is an ineffective means of determining terroristic threat).

155. Lizza, *supra* note 65.

156. *See supra* Part II.B.

screening processes[157] as well as screening through social norms and behavior control.[158] These screening processes would often require governments or their private delegates to screen individuals on the basis of race, and any failure to do so would often carry legal consequences as well as social penalties such as ostracization.[159]

### *C. Cyberarchitecture of Algorithmic Jim Crow*

Perhaps the easiest way to understand how the Jim Crow regime is being replicated in a big data world through Algorithmic Jim Crow is to consider the following scenario: imagine substituting race-based classifications with classifications of digitally derived suspiciousness. Rather than relying upon a targeted class, such as race, national origin, gender, or religion, as a sole basis for exclusion, big data allows for exclusion to be based on an abstraction, such as digitally inferred or algorithmically anchored guilt or suspicion.[160] In addition, big data can aggregate protected classifications with other collected data.[161] For example, biometric screening that uses soft biometric indicators, such as digital assessments of skin color and estimated age extracted from a digital photo, can combine race data proxies with other proxy variables to predict criminal or terroristic behavior (e.g., aggregating passport number and digital photo with data analysis of web browsing activity and social media presence).[162] In addition, there are multiple components to extreme vetting, including, but not limited to, biometric identification,[163] record linkage,[164] information extraction,[165] and predictive analytics.[166] In some circumstances, these technologies allow for classification and then screening. In other circumstances, these technologies allow for just the opposite: screening, then classification.

What is difficult to understand is how machine learning and artificial intelligence can replace human judgment in the classification and screening processes of Algorithmic Jim Crow regimes. In a small data world, Jim Crow required a human to physically inspect the skin color of an individual to determine the race of that individual (e.g., a physician attesting to the race of an individual on a birth certificate).[167] In the small data world, screening

157. *See supra* Part II.B.
158. *See supra* Parts II.A–B.
159. *See* KENNEDY, *supra* note 105, at 206.
160. *See, e.g.*, Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1759 (2015).
161. *Id.*
162. *See, e.g.*, Shanti Gomatam & Michael D. Larsen, *Record Linkage and Counterterrorism*, 17 CHANCE 1, 25–29 (2004).
163. *See supra* Introduction; *see also* VACCA, *supra* note 37, at 589 (stating that biometrics is "[t]he science of automatic identification or identity verification of individuals using physiological or behavioral characteristics").
164. Michael D. Larsen, *Record Linkage, Nondisclosure, Counterterrorism, and Statistics*, STAT. SOC. CAN. (May 2006), https://ssc.ca/sites/ssc/files/survey/documents/SSC2006_Michael_Larsen.pdf [https://perma.cc/P3ZF-8URC] (explaining that record linkage seeks to identify records that belong to the same individual).
165. *Id.*
166. *See supra* note 51 and accompanying text.
167. *See supra* Part II.A.

processes also required human judgment (e.g., a county clerk inspecting birth certificates before issuing marriage licenses and marriage certificates to determine compliance with antimiscegenation laws).[168]

In contrast, human involvement is not required to classify individuals in a big data world. An individual can be classified as a potential criminal, terrorist, or threat risk based on digital data alone and digitized analysis such as algorithmic screening. Algorithmic tools can analyze data to establish identity (e.g., a record-locator matching algorithm such as database screening systems that match names with passport numbers and other databases of personally identifiable information) and screen for suspicious digital profiles (e.g., combine passport information with stored data and real time data).[169] Stored data might include bulk telephony metadata[170]—databases that collect time, duration, and geolocation of calls—and other government records and private data, such as consumer activities.[171] Real-time analytics can include situational awareness systems that attempt to analyze real-time video surveillance feeds that connect the monitored individual through facial recognition technology to that individual's social media.[172]

Hence, the nature of classification and screening capacities are radically different in a big data world. Classification, therefore, can be based in part or in whole on artificial intelligence. Similarly, screening in a big data world does not rely on human processes. The No Fly List, for example, can be generated through database screening and digital watchlisting systems rather than human nomination.[173] Thus, in a big data world, classification and screening protocols can be combined, digitized, and automated. As a result, these big data classification and screening systems may be nearly impossible for a citizen to interrogate or challenge.[174]

What is similar between big data and small data exclusionary regimes is that separation and segregation is at the heart of the processes. What appears

168. *See supra* Part II.A.

169. *See, e.g.*, Gomatam & Larsen, *supra* note 162.

170. *See, e.g*, *supra* note 54 and accompanying text.

171. *See generally* Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773 (2015).

172. *See* Jonah Engel Bromwich et al., *Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says*, N.Y. TIMES (Oct. 11, 2016), https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html [https://perma.cc/C2TJ-NCWX]; Matthew Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU: FREE FUTURE (Oct. 11, 2016, 11:15 AM), https://www.aclu.org/blog/free-future/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed [https://perma.cc/7X44-WEPA]; Ally Marotti, *Chicago Police Used Geofeedia, the TweetDeck for Cops Under Fire from ACLU*, CHI. TRIB. (Oct. 13, 2016), http://www.chicagotribune.com/bluesky/originals/ct-geofeedia-police-surveillance-reports-bsi-20161013-story.html [https://perma.cc/566Y-HBZK]; Nicole Ozer, *Police Use of Social Media Surveillance Software Is Escalating, and Activists Are in the Digital Crosshairs*, ACLU: FREE FUTURE (Sept. 22, 2016, 2:45 PM), https://www.aclu.org/blog/free-future/police-use-social-media-surveillance-software-escalating-and-activists-are-digital [https://perma.cc/NG4Y-GD33].

173. Hu, *supra* note 160, at 1761–62.

174. *See generally* United States v. Esquivel-Rios, 725 F.3d 1231 (10th Cir. 2013); Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981 (2014); Hu, *supra* note 160.

to be—at the earliest stages of the big data governance phenomenon—purely national security motivated protocols, such as the No Fly List, might not appear to be a part of a larger segregationist regime. At the earliest stages of Jim Crow, separation of the races was deemed necessary by the Court in *Plessy v. Ferguson*[175] under security rationales to avoid race-based conflict.[176] At the earliest stages of Algorithmic Jim Crow, isolating individuals based on data suspicions is also justified under security rationales—to prevent terrorism.

Unlike historic Jim Crow, established to continue a racial hierarchy first instituted through slavery, big data regimes do not overtly seek to create subordinate social classes. But that may well be the result. Like under historic Jim Crow regimes, security needs are professed as justification. Even if we are not yet faced with a mature Algorithmic Jim Crow regime, it is important to recognize that Jim Crow laws took decades to develop into a pervasive legal system.[177] With the benefit of hindsight, we now examine the full arc of Jim Crow, including the opportunity to revisit the legal precedent that allowed for segregation to take root and become normalized.[178] Jim Crow did not commence with the segregation of every water fountain, swimming pool, bus, train, movie theater, hotel, or restaurant.[179] Jim Crow did, however, eventually convert nearly every citizen into a race classification expert and screening specialist to comply with the laws.[180] Jim Crow laws imposed a duty under law or social norms upon many entities—public, private, and individual citizens—to classify and screen.[181]

How will classification and screening under Algorithmic Jim Crow, like historic Jim Crow, require classification and screening requirements under the law? How will Algorithmic Jim Crow impose a legal duty upon public, private, and individual citizens to classify and screen? Jim Crow laws mandated paper-based classifications such as attestation to racial classifications on birth certificates.[182] Big data technologies, however, do not require discrete screening or classification procedures because of the nature of modern data tools. Instead of separate processes that treat screening and classification as separate, big data tools have the capacity to execute both simultaneously.

In a small data world, linearity was more common between classification and screening: the former had to follow the latter as a matter of logic. Without racial classification, racial screening would not have been possible. Once an individual had been classified as white, privileges under Jim Crow logically followed that racial status. With big data, assessments can be made

175. 163 U.S. 537 (1896), *overruled by* Brown v. Bd. of Educ., 347 U.S. 483 (1954).
176. *Id.* at 559.
177. *See* TISCHAUSER, *supra* note 105, at 1.
178. *See supra* Part II.A.
179. *See supra* Part II.A.
180. *See supra* note 159 and accompanying text.
181. *See supra* Part II.A.
182. *See supra* note 128 and accompanying text (discussing Form 59-3-17-24-65M, titled "Registration of Birth and Color–Virginia").

concurrently and, thus, consecutive processes are not necessary but may occur. Under big data theories of identity management, an aggregation of data can, for instance, map identity—such as classification of potential terrorist status. In addition, the same vetting and screening protocols facilitate determinations as to access (e.g., whether an individual can board a plane or enter the country). It is the accumulation and analysis of the ever-growing aggregation of data that makes possible the database screening and algorithmic decision-making that is at the core of the extreme vetting enterprise.

New classification and screening technologies thus eliminate or reduce the need to conduct human-based screening. Historic Jim Crow laws required bus drivers to segregate passengers on the basis of race, a screening protocol that required human judgment and human action.[183] Contemporary systems may use a combination of automated screening and human screening, such as TSA screeners relying upon the predictive analytic systems of the No Fly List.[184] Algorithmic Jim Crow may also facilitate fully automated and digitized screening systems.[185]

Under contemporary forms of big data governance, classification will likely comprise a combination of traditional characteristics such as well-recognized protected classifications (e.g., race, national origin, gender, and age) as well as nonprotected attributes (e.g., data deemed suspicious, unstable or anomalous digital data, and database screening and algorithmically derived results) that allow for inferences of guilt. But instead of impermissibly distributing or withholding privileges based on protected classifications, big data will simply incorporate them as part of a "risk assessment." Such threat risk assessments will attempt to predict criminal or terroristic predisposition.[186] Unlike historic Jim Crow, Algorithmic Jim Crow may not require classification in order to conduct screening. Because of the vast amounts of digital data that can be analyzed for both classification and screening purposes, data will, at times, be collected and sorted for classification to screen.[187] At other times, data will be collected and screened

183. *See generally supra* Parts II.A–B.

184. *See* Hu, *supra* note 160, at 1743.

185. *Id.* at 1746.

186. *See infra* note 227 and accompanying text; *see also* David Cole, *The Difference Prevention Makes: Regulating Preventive Justice*, 9 CRIM. L. & PHIL. 501, 504 (2014); Jennifer C. Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327, 331 (2014).

187. Emerging facial recognition technology can capture digital photos and screen for "soft biometrics" that include data relevant to the classification of protected individuals—such as identifying ethnicity and skin color. *See* Noah Shachtman, *Army Tracking Plan: Drones That Never Forget a Face*, WIRED (Sept. 28, 2011, 6:30 AM), https://www.wired.com/2011/09/drones-never-forget-a-face/ [https://perma.cc/8HLQ-TFJ4] ("The key [to more advanced facial recognition technology] is a kind of digital stereotyping. Using a series of so-called 'soft biometrics'—everything from age to gender to 'ethnicity' to 'skin color' to height and weight—the system can keep track of targets 'at ranges that are impossible to do with facial recognition' . . . ."); *see also* SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS 110 (2015) ("Digital epidermalization [through biometric recognition technologies] is the exercise of power cast by the disembodied gaze of certain surveillance technologies (for example, identity card readers and e-passport verification machines) that can

to determine a classification. Thus, big data governance facilitates screening and classification, or classification and screening, through big data systems such as database screening, digital watchlisting, and security analytics.

Extreme vetting, as proposed in the March 6, 2017, Order and the September 24, 2017, Order—and as promulgated by other immigrant screening systems—is used in this Article as a mere example for how Algorithmic Jim Crow regimes can potentially burrow into national security policy-making. Directives such as the presidential Executive Order[188] can create classification and screening systems under law, regulation, and policy.[189] To understand how, it is important to dissect the manner in which extreme vetting and other DHS algorithmically driven programs are likely to classify and screen citizens and noncitizens.

Yet, a full explanation of how algorithmic classification and screening systems work, and the problems presented by big data and predictive analytics, is beyond the scope of this Article.[190] There has been much important work and attention addressing the broader topic, as well as the issue of discrimination resulting from the use of these emerging technologies.[191] Predictive analytics make actionable or useful information from data by using algorithms and other machine-learning techniques.[192]

---

be employed to do the work of alienating the subject by producing a truth about the racial body and one's identity (or identities) despite the subject's claims.").

188. *See supra* Part I.

189. *Id.*

190. Important scholarship and research is underway on the topics of algorithmic governance, and algorithmic fairness and transparency. *See generally* Mike Ananny & Kate Crawford, *Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability*, NEW MEDIA & SOC'Y, Dec. 13, 2016; Omer Tene & Jules Polonetsky, *Taming the Golem: Challenges of Ethical Algorithmic Decision Making*, 19 N.C. J.L. & TECH. (forthcoming 2017), https://ssrn.com/abstract=2981466 [https://perma.cc/HTN5-24SG]; Solon Barocas et al., Governing Algorithms: A Provocation Piece (2013) (unpublished manuscript), http://edshare.soton.ac.uk/8849/31/48-Governing-Algorithms.pdf [https://perma.cc/R9R9-N4HW]; Harry Surden, Values Embedded in Legal Artificial Intelligence (Mar. 13, 2017) (unpublished manuscript), https://ssrn.com/abstract=2932333 [https://perma.cc/ZD8K-JA3G].

191. *See generally* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION (2016) (providing examples of discrimination from the use of predictive modeling in a variety of settings); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015); Anupam Chander, *The Racist Algorithm?*, 115 MICH. L. REV. 1023 (2017); Tal Zarsky, *Transparency in Data Mining: From Theory to Practice*, *in* DISCRIMINATION AND PRIVACY IN THE INFORMATION SOCIETY: DATA MINING AND PROFILING IN LARGE DATABASES 301 (Bart Custers et al. eds., 2013); Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017); Claire Cain Miller, *Algorithms and Bias: Q. and A. with Cynthia Dwork*, N.Y. TIMES (Aug. 10, 2015), https://www.nytimes.com/2015/08/11/upshot/algorithms-and-bias-q-and-a-with-cynthia-dwork.html [https://perma.cc/93EH-9G5N] ("Cynthia Dwork, a computer scientist at Microsoft Research in Silicon Valley . . . discussed how algorithms learn to discriminate, who's responsible when they do, and the trade-offs between fairness and privacy."); Lauren Weber & Elizabeth Dwoskin, *Are Workplace Personality Tests Fair?*, WALL ST. J. (Sept. 29, 2014), https://www.wsj.com/articles/are-workplace-personality-tests-fair-1412044257 [https://perma.cc/3GUY-F7ZP].

192. Ravi Kalakota, *Making Money on Predictive Analytics—Tools, Consulting and Content*, BUS. ANALYTICS 3.0 (Mar. 18, 2012), https://practicalanalytics.co/2012/03/18

While algorithms and other machine-learning technologies can make meaningful connections from large sets of data that are outside any human capabilities, researchers and experts are increasingly noting their limitations: artificial intelligence systems are not immune to inherent racial biases, and thus judgments derived from algorithms may also be suspect.[193]

## III. THEORETICAL EQUALITY UNDER ALGORITHMIC JIM CROW

Part III explores how modern vetting protocol is properly understood as part of a web of identity-management technologies that may extend to the entire citizenry. For example, although extreme vetting is presented as a procedure that is restricted to refugees, immigrants, and foreign visitors seeking a travel visa to the United States, this characterization is misleading. Extreme vetting is better grasped as a function of database screening and digital watchlisting systems that can be applied equally to all citizens and noncitizens under a wide range of contexts, often justified by national and homeland security policy rationales.

### *A. Limitations of Equal Protection as a Legal Response to Algorithmic Jim Crow*

Before they are allowed to fly, work, drive, or vote, citizens and noncitizens alike can now be subjected to mass data collection and automated or semiautomated database screening protocols.[194] Increasingly, in the name of national and homeland security, post-9/11 big data programs implemented by the government allow for core rights and freedoms to be partially obstructed in some instances or altogether blocked in others.[195] Moreover, because of the "virtual" nature of mass data collection and database screening and the classified nature of certain programs, the digital mediation and potential interference of liberty interests can occur without our knowledge or consent.[196]

As the national population is increasingly represented in the growing databases and becomes subject to potential across-the-board vetting and screening, claims of equal protection violations may collapse. This

/making-money-on-predictive-analytics-tools-consulting-and-content/ [https://perma.cc/LBV3-N9BL].

193. *See generally* O'NEIL, *supra* note 191; DAVID ROBINSON ET AL., CIVIL RIGHTS, BIG DATA, AND OUR ALGORITHMIC FUTURE (2014); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016); Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/EM5U-ZNTA]; Miller, *supra* note 191.

194. *See infra* notes 327–33 and accompanying text.

195. *See Big Data: Seizing Opportunities, Preserving Values*, WHITE HOUSE 5 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf [https://perma.cc/R9S9-S9HB].

196. *See* PASQUALE, *supra* note 191, at 101–03 (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) (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).

likelihood increases as defenders of database screening argue such screening minimizes the role of the human element and thus minimizes the risk of racial profiling on a theoretical level. Because the algorithms of any given big data vetting or database screening system will not be transparent to those subject to screening, the denial of a benefit or privilege, or consequences such as detainment and deportation, will be without apparent cause beyond the fact that the database has determined that they should be targeted.[197]

Thus, Algorithmic Jim Crow demonstrates how Jim Crow regimes can adapt and evolve through use of modern technology. In Michelle Alexander's seminal work, *The New Jim Crow: Mass Incarceration in the Age of Colorblindness*,[198] the story of Jim Crow has transformed from one of mass segregation and disenfranchisement regimes in the post-Reconstruction era into mass incarceration regimes in the post-War on Drugs[199] and the era of mandatory minimum sentencing guidelines.[200] Alexander posits that Jim Crow should be evaluated as a constantly evolving process, not a historical artifact.[201] Redressing new forms of Jim Crow requires observing innovations in law and policy that result in the entrenchment of inequities on the basis of race and other sites of historic discrimination.[202] As such, Alexander warns that vigilance is needed to bear witness to an evolutionary process of law and policy that can lead to new caste systems.[203] This is especially true in a modern era that may present the mechanism for the caste as colorblind,[204] and involve data tracking and digital sorting methods that may present a "virtual" cage problem.[205]

Taking a cue from Alexander to refuse to limit Jim Crow to regimes designed to subordinate a single race or class of individuals, we may see the newest emergence of Jim Crow in mass surveillance and algorithm-driven decision-making. Database screening and digital watchlisting systems, in fact, can serve as complementary and facially colorblind supplements to mass incarceration systems.[206] The purported colorblindness of mandatory sentencing and mass incarceration systems, for instance, parallels the

197. *See* Hu, *supra* note 160.

198. MICHELLE ALEXANDER, THE NEW JIM CROW: MASS INCARCERATION IN THE AGE OF COLORBLINDNESS (rev. ed. 2012).

199. *Id.* at 47–58, 185–86.

200. *Id.* at 87–93.

201. *See generally id.*

202. *Id.* at 58.

203. *Id.* at 21 ("Any candid observer of American racial history must acknowledge that racism is highly adaptable. The rules and reasons the political system employs to enforce status relations of any kind, including racial hierarchy, evolve and change as they are challenged.").

204. *Id.* at 240–45.

205. *Id.* at 184 ("In the system of mass incarceration, a wide variety of laws, institutions, and practices—ranging from racial profiling to biased sentencing policies, political disenfranchisement, and legalized employment discrimination—trap African Americans in a virtual (and literal) cage."); *see also* Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321, 1328 (2008).

206. *See* BROWNE, *supra* note 187, at 110; Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 329 n.6 (2015).

purported colorblindness of mandatory database screening and vetting systems.

As Reva Siegel has theorized, anticlassification jurisprudence cannot achieve the same aims as antisubordination or antibalkinization jurisprudence.[207] In contemporary equality cases considered before the Supreme Court, Siegel observes: "The Justices who vote against affirmative action and other race-conscious civil rights policies are said to reason from a colorblind anticlassification principle, premised on the belief that the Constitution protects individuals, not groups, and so bars all racial classifications, except as a remedy for specific wrongdoing."[208] This judicial predisposition to overturn programs that redress wrongs for suspect classifications—even when the clear purpose of such programs is to assist those historically harmed by such classifications—means that vetting and screening protocols that do not overtly target such suspect classifications will not present an equal protection problem. In other words, if the "anticlassification principle" continues to dominate equal protection jurisprudence, "race-neutral" and equally applied database screening and digital watchlisting systems will not appear to be inconsistent with the anticlassification premise of equality law. Therefore, such programs may pass equal protection muster, even if they impose disparate consequences.[209]

Similarly, Jack Balkin provocatively asserts that the law of equality is often, in fact, the law of inequality.[210] Balkin argues that, historically and paradoxically, the law of equality has been adaptive to enforce inequality.[211] Balkin explains that the Supreme Court in *Plessy v. Ferguson* acknowledged that a multitude of social and economic inequities arise on the basis of race.[212] Nonetheless, *Plessy* ratified racial segregation after finding no equal protection defect with Jim Crow institutions.[213] The Court concluded that

207. Reva B. Siegel, *From Colorblindness to Antibalkanization: An Emerging Ground of Decision in Race Equality Cases*, 120 YALE L.J. 1278, 1282 (2011) (contending that equality law can and should strive toward "vindicating antibalkanization—rather than colorblindness—values").

208. *Id.* at 1281.

209. *Id.* at 1338–42 (explaining that disparate-impact theories of discrimination are more currently and directly recognized by equality jurisprudence established under Title VII of the Civil Rights Act of 1964). *See generally* MICHAEL OMI & HOWARD WINANT, RACIAL FORMATION IN THE UNITED STATES (3d ed. 2015); Reva B. Siegel, *Why Equal Protection No Longer Protects: The Evolving Forms of Status-Enforcing State Action*, 49 STAN. L. REV. 1111 (1997).

210. JACK M. BALKIN, CONSTITUTIONAL REDEMPTION: POLITICAL FAITH IN AN UNJUST WORLD 139–73 (2011).

211. *Id.* at 163 ("The model of scrutiny rules declares unconstitutional a set of delegitimated state practices of race discrimination that were associated with Jim Crow in the South, but it does not abolish all forms of racial inequality or social stratification. Rather, the model of scrutiny rules develops alongside new forms of racial and social stratification produced in the post-civil rights era."); *see also* Reva B. Siegel, *Discrimination in the Eyes of the Law: How "Color Blindness" Discourse Disrupts and Rationalizes Social Stratification*, 88 CALIF. L. REV. 77, 83 (2000) (describing a process of "preservation-through-transformation" whereby the law adapts to protect new forms of social stratification).

212. BALKIN, *supra* note 210, at 145–46 (citing Plessy v. Ferguson, 163 U.S. 537, 551–52 (1896), *overruled by* Brown v. Bd. of Educ., 347 U.S. 483 (1954)).

213. *Id.* at 144–46.

the "separate but equal" principle upheld the equality guarantees required under the Equal Protection Clause so long as the government provided a form of theoretical equality on the back end of segregation.[214] According to *Plessy*, the separation of the races on the front end of state laws did not create a violation of the Equal Protection Clause because the discrimination could be redressed on the back end.[215] The *Plessy* Court further concluded that racial separation on the front end could serve important law-and-order goals, such as increasing a state's interest in ensuring safety and social order among the different races.[216]

This legal reasoning is now widely discredited and, as noted, the Court now has an antidiscrimination approach that strictly scrutinizes laws that operate along such suspect classifications.[217] Nevertheless, that approach too is viewed as inadequate by constitutional law experts and as hindering efforts to address unequal realities. In contrast to the theoretical equality guarantees assured on the back end of sorting methods instituted under historic Jim Crow regimes, at the dawn of the big data revolution we may be witnessing more and more legal contexts in which all are equally subject to digitalized vetting and database screening protocols but with results on the back end that raise equal protection concerns. Equality law that demands that the government provide equal treatment under the law on a theoretical level on the front end therefore prohibits traditional Jim Crow institutions. But Siegel, Balkin, and others caution that equality law cannot stop at a judicial inquiry that ensures colorblindness on the front end since that risks turning a blind eye to the disparate impacts that can result on the back end.[218]

As the government continues to acquire more big data tools to serve governance goals, such as database screening systems and predictive analytics that assess risk, equality law may find no constitutional problem with replication in reverse form of the social inequality permitted under the "separate but equal" principle. Under an emerging technologically enhanced Jim Crow regime, mass surveillance and semiautomated or automated algorithmic sorting methods will appear to be equally applied across entire populations. The colorblind and anticlassification premises of vetting and screening systems will comport with an "equal but separate" principle. These systems, however, will potentially offer only theoretical equality on the front end of newly emerging data surveillance and data-sorting methods. Meanwhile, any disparate impacts on the back end will be hard to challenge judicially because algorithmic decision-making can occur in ways that are difficult to document.

---

214. *Id.* at 140.

215. *Id.* 144–48 (describing a "tripartite theory" of divided rights and equality that recognized three categories: "civil, political, and social"). *Plessy* did not attempt to extend political or social equality rights under the Fourteenth Amendment. *Id.*

216. *Plessy*, 163 U.S. at 550–51.

217. *See generally supra* Part II.A.

218. *See* Primus, *supra* note 26, at 504–09.

The evolution of constitutional protections is, thus, critically necessary in what Balkin and Sanford Levinson term the "National Surveillance State."[219] In the National Surveillance State, the integration of bureaucratized and normalized data collection and Information Society surveillance technologies into day-to-day governance should be understood as a distinctive concern of American constitutionalism: "One of the most important developments in American constitutionalism is the gradual transformation of the United States into a National Surveillance State."[220] Constitutional protections that once were taken for granted in a small data world have proven robust in theory but lacking in practical application.[221] Often, it is not so much that our physical personhood is threatened in the National Surveillance State, but as Daniel Solove describes it, it is our "digital person" that has been placed at risk.[222]

The shift to the National Surveillance State and big data governance should be understood as paradigmatic. Big data and algorithmic intelligence technologies are disruptive and transformative in nature.[223] Defined by their predictive and correlative capacities, big data technologies are capable of facilitating a new type of knowledge that some argue is akin to virtual reality (e.g., probabilistic or algorithmic holograms).[224]

Thus, big data surveillance that transforms into normalized day-to-day governance practices often poses harms that are more virtual than physical—for instance, digitally derived suspicion harms rather than detention harms.[225] As a result, big data-driven predictive-policing methods are void of reasonable suspicion as once defined in a small data world.[226] For example, while in a small data world, reasonable suspicion is based on specific facts or inferences regarding a specific individual's involvement in criminal activity. In a big data world, on the other hand, targeting of suspects can proceed based on data that is associated with them as collected in a database

219. *See* Balkin & Levinson, *supra* note 145, at 521. Balkin and Levinson define 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." *Id.* at 520–21; *see also* Balkin, *supra* note 145, at 3.

220. Balkin & Levinson, *supra* note 145, at 520.

221. *Id.* at 523.

222. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1 (2004); *see also* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 1 (2012).

223. *See generally* KITCHIN, *supra* note 32; MAYER-SCHÖNBERGER & CUKIER, *supra* note 32; EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM (2013); danah boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15 INFO. COMM. & SOC'Y 662 (2012); Citron & Pasquale, *supra* note 196; Hu, *supra* note 171; Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63 (2012).

224. *See* Seth Fletcher, *How to Think About Privacy: An Interview with Jason Lanier*, SCI. AM. (Nov. 1, 2013), https://www.scientificamerican.com/article/lanier-interview-how-to-think-about-privacy/ [https://perma.cc/AJ5J-5MVT].

225. *See* Murphy, *supra* note 205, at 1358.

226. *See* Ferguson, *supra* note 206, at 336; Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 42–48, 56 (2014).

and that fit particular profiles targeted by database searches. Small data discrimination, consequently, can evolve into a form of big data discrimination in a myriad of ways. For example, statistical guilt or correlative evidence that support inferences of suspicion can be assigned through "race-neutral" tools that screen entire populations "equally."

### *B. No Fly List and Discrimination on the Back End of Vetting and Database Screening Protocols*

To further understand how Algorithmic Jim Crow works in practice in across-the-board vetting, this Part examines the No Fly List, the birth of a "precrime"[227] vetting system that screens citizens and noncitizens in a purportedly equal manner on the front end. De facto discrimination, for instance, has been alleged in the disparate impact of the No Fly List, a system that has been referred to as a "Flying While Muslim" program.[228]

Although discrimination may not occur on the front end of the vetting and screening process of the No Fly List, plaintiffs challenging the No Fly List allege that the program results in disparate consequences that disproportionately impact those populations associated with terrorism, such as military-age Muslim males[229] or Muslims who may be swept into the No Fly List database screening systems by virtue of intensified surveillance of Muslim communities by the intelligence community.[230] Examining the No Fly List litigation shows that, in the absence of discrimination in front-end enforcement techniques, back-end discrimination can emerge from the supposedly neutral analytics of the digital watchlisting and database screening system itself.

The No Fly List as well as other vetting and screening systems have already faced multiple legal challenges. Federal courts have been asked to address the new types of harms presented by digital watchlisting and database screening in the National Surveillance State.[231] Of the challenges to multiple identity-management technologies that have reached the Supreme Court, none have allowed for an equal protection claim. As Cass Sunstein explains, "[t]he Equal Protection Clause is directed at the legality of classifications. When a classification is challenged, the first question is whether it is drawn on the basis of race or some other characteristic thought to call for

227. *See* 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, 93 (Mireille Hildebrandt & Katja de Vries eds., 2013); *see also* Cole, *supra* note 186, at 518; Daskal, *supra* note 186, at 328.

228. *'Flying While Muslim': Profiling Fears After Arabic Speaker Removed from Plane*, NPR (Apr. 20, 2016), http://www.npr.org/2016/04/20/475015239/flying-while-muslim-profiling-fears-after-arabic-speaker-removed-from-plane [https://perma.cc/K6CS-3DA3].

229. The plaintiffs in *Latif v. Holder* included many military-age Muslim males, many of whom are U.S. citizens who served in the U.S. military. *See, e.g.*, First Amended Complaint at 1, Ibrahim v. Dep't of Homeland Sec., 62 F. Supp. 3d 909 (N.D. Cal. 2014) (No. 3:06-00545-WHA), 2006 WL 2330786.

230. Ibrahim was under surveillance by the FBI, allegedly because she was Muslim. *See Ibrahim*, 62 F. Supp. 3d at 916–17, 929.

231. *See generally* Balkin & Levinson, *supra* note 145.

'heightened' scrutiny."[232] If there is an impermissible classification, that statute must survive the appropriate level of scrutiny. If there is no classification, Sunstein explains, the inquiry proceeds to a second question:

> Was the classification motivated by an 'intention' to treat some class differently on the basis of race or, again, any other characteristic said to call for heightened scrutiny? If the answer is affirmative, heightened scrutiny must be applied; if negative, the statute must be upheld unless it is not rationally related to a legitimate state interest.[233]

Under the vetting and screening protocols of the No Fly List, there is no classification or characteristic that warrants "heightened" scrutiny. Further, thus far, there is no evidence that the vetting and database screening protocol is motivated by an "intention" to discriminate on the basis of an impermissible classification. Because equal protection is not a viable option to challenge the No Fly List—as the screening is applied in a purportedly equal manner—the use or misuse of data-driven tools has been central to the inquiry in the federal courts.

Specifically, No Fly List litigation has been primarily successful through procedural due process claims, though many plaintiffs also originally raised substantive due process claims.[234] The due process challenge to the No Fly List is relevant here because that challenge attacks the workings of the vetting and screening processes, and, importantly, how identity-management technology can lead to stigmatization and reputational harms, allegedly on the basis of classification. For the purposes of this discussion, therefore, it is helpful to concurrently examine the due process analysis of two similar No Fly List cases, though acknowledgeable differences exist between them.

In both *Ibrahim v. Department of Homeland Security*[235] and *Latif v. Holder*,[236] federal courts analyzed due process claims that the plaintiffs' rights to travel were infringed upon by their inclusion on the No Fly List. In *Latif*, the plaintiffs argued that the No Fly List burdens a protected liberty interest[237] without due process of law: namely, that their placement on the No Fly List burdened their liberty interests in the freedom of travel,[238] and freedom from the false stigmatization and association with terrorists and

232. Cass R. Sunstein, *Public Values, Private Interests, and the Equal Protection Clause*, 1982 SUP. CT. REV. 127, 127; *see also* United States v. Virginia, 518 U.S. 515, 533 (1996); Regents of the Univ. of Cal. v. Bakke, 438 U.S. 265, 290–91 (1978); Frontiero v. Richardson, 411 U.S. 677, 686–87 (1973) (plurality opinion) (Brennan, J.); Loving v. Virginia, 388 U.S. 1, 11 (1967); Brown v. Bd. of Educ., 347 U.S. 483, 493 (1954); Bertrall L. Ross II & Su Li, *Measuring Political Power: Suspect Class Determinations and the Poor*, 104 CALIF. L. REV. 323, 324–26 (2016) (discussing evolution of suspect classifications and more exacting judicial levels of scrutiny for specific groups deemed protected under the Equal Protection Clause of the Fourteenth Amendment).

233. Sunstein, *supra* note 232, at 127–28.

234. *See infra* notes 235–40 and accompanying text.

235. 62 F. Supp. 3d 909 (N.D. Cal. 2014).

236. 28 F. Supp. 3d 1134 (D. Or. 2014).

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

238. The Supreme Court has recognized both a right to "freedom of movement" and a right to international travel. *See, e.g.*, Kent v. Dulles, 357 U.S. 116, 125–26 (1958).

terroristic activities implicit in inclusion on the No Fly List.[239] Similarly, the plaintiff in *Ibrahim* alleged deprivations of her liberty and property interests without due process of law.[240]

Once a protected liberty interest in either the travel or reputational interest was established, in each case, the plaintiffs were required to satisfy the three-part due process test set forth in *Mathews v. Eldridge*.[241] Under *Mathews*, the court weighs: (1) "the private interest that will be affected by the official action"; (2) "the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards"; and (3) "the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail."[242]

For example, under the first *Mathews* factor in *Latif*, the plaintiffs contended that protected liberty interests reside in freedom of travel and movement, and in reputational concerns.[243] Under the second factor, the plaintiffs argued that the redress procedure inherently risks an unacceptably high error rate because it does not allow plaintiffs, or other individuals placed on the No Fly List, the opportunity to confront or rebut any evidence used in determining the appropriateness of their placement on the list.[244] In other words, the vetting and screening protocol of the No Fly List allowed for discrimination on the back end in that those singled out as potential threats had no meaningful redress. Finally, regarding the third factor, although national security is a significant government interest, the procedural protections provided to plaintiffs were insufficient given the lack of notice and "wholly ineffective" procedures of the protocol.[245]

The No Fly List due process challenges are necessary to challenge back-end discrimination because there is no other way to interrogate the classification mechanism used to assess threat risk or what data might be deemed suspicious. In other words, there may be alleged commonalities among those finding themselves on the No Fly List, such as being Muslim American, Arab American, a citizen of a Muslim-majority country, or of Middle Eastern descent. Because the government argues that the No Fly List involves classified information—including database screening systems and vetting protocols that make "predictive judgments"—there is no meaningful way to interrogate how and why that characteristic predominates among those selected by the algorithm or digital watchlisting technology.[246]

239. Complaint at 50–51, *Latif*, 28 F. Supp. 3d 1134 (No. 10-CV-750-BR).

240. First Amended Complaint at 11–12, *Ibrahim*, 62 F. Supp. 3d 909 (No. C06-0545 WHA), 2006 WL 2330786.

241. 424 U.S. 319 (1976).

242. *See id.* at 335.

243. *Latif*, 28 F. Supp. 3d at 1147–48.

244. *Id.* at 1152.

245. *Id.* at 1160–61.

246. *See* Defendants' Cross-Motion for Summary Judgment at 18, *Latif*, 28 F. Supp. 3d 1134 (No. 3:10-cv-00750-BR), 2015 WL 11347548 (arguing that the No Fly List is designed to make a "predictive judgment" of potential threats).

The closest plaintiffs on the No Fly List have come to determining whether and how they faced classification-based discrimination is through a deconstruction of the digital watchlisting architecture and an analysis of the databases that may be implicated in the vetting and screening protocols.[247] The complaints and trial records appear to suggest that the No Fly List results in a disparate impact.[248] The algorithms and databases present themselves as neutral, without bias. Thus, due process protection allows for some interrogation of the vetting and database screening systems and its errors.

Human error can become unimpeachable truth but for legal challenges. Database error risks a form of unimpeachable truth without a legal theory to challenge it. What are the reasons for being wrongly placed on the No Fly List? How does one prove discriminatory animus in vetting and screening protocols? How does one establish algorithm-derived discrimination? The No Fly List litigation shows that equal protection as a theory fails to shield those suffering disparate treatment or de facto back-end discrimination under the current framework for evaluating Fourteenth Amendment claims.

As in *Plessy*, Algorithmic Jim Crow may offer theoretical equality that may thwart challenges under the Equal Protection Clause. As in *Korematsu*, governmental action taken purportedly in defense of national security may be viewed as legitimately containing risk and may not be construed as targeting individuals on the basis of classification. *Plessy* and *Korematsu* represent two discredited cases that are now considered a part of what Richard Primus and other scholars refer to as the "anti-canon" of constitutional law.[249] Just as those challenging the constitutionality of historic Jim Crow regimes in *Plessy* and Japanese internment in *Korematsu* were unsuccessful, those challenging Algorithmic Jim Crow regimes may face similar difficulties due to similar deficiencies in current jurisprudence.

## IV. FUTURE OF ALGORITHMIC JIM CROW

To further illustrate how screening and vetting protocols can be extended to the entire citizenry, Part IV examines how the Supreme Court has handled challenges to multiple identity-management programs in recent years. Parties in several cases are attempting to seek judicial review of government identity-management programs and dataveillance technologies, programs that are rapidly flourishing in both scope and number. The Supreme Court has now had the opportunity to review multiple identity-management

247. *See id.*

248. Various plaintiffs have alleged in litigation that constitutional harms arise from big data watchlisting and dataveillance or cybersurveillance targeting systems, including database screening systems. *See, e.g.*, Latif v. Holder, 686 F.3d 1122, 1124, 1126 (9th Cir. 2012) (noting that plaintiffs alleged due process violations in relation to the No Fly List); Afifi v. Lynch, 101 F. Supp. 3d 90, 95–96 (D.D.C. 2015) (noting that plaintiffs alleged Fourth Amendment violations based on cybersurveillance GPS tracking).

249. Richard A. Primus, *Canon, Anti-Canon, and Judicial Dissent*, 48 DUKE L.J. 243, 243 (1998); *see also* Akhil Reed Amar, Plessy v. Ferguson *and the Anti-Canon*, 39 PEPP. L. REV. 75, 75 (2011); J.M. Balkin & Sanford Levinson, *The Canons of Constitutional Law*, 111 HARV. L. REV. 963, 984–95, 1014–19 (1998); Jamal Green, *The Anticanon*, 125 HARV. L. REV. 379, 379 (2011).

systems in *NASA v. Nelson*,[250] *Chamber of Commerce v. Whiting*,[251] and *Arizona v. United States*.[252] In each of these cases, however, the equal protection consequences of the vetting protocols were not before the Supreme Court.

### *A. Biometric Credentialing and Vetting Protocols:* NASA v. Nelson

*Nelson*[253] involved a challenge to aspects of Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (the "HSPD-12" program)[254] in an effort to limit the impact of this identity-management program on personal privacy rights.[255] HSPD-12 is a post-9/11 presidential directive promulgated by the Bush administration to implement a biometric ID-credentialing and background-check program for federal employees and federal contractors. HSPD-12 and the litigation surrounding *Nelson* provide an opportunity to examine the impact of identity-management technologies. It explores some future implications of these technologies, including the possibility of morality testing in civilian background tests, which was originally at issue in the case.

Exploring the impact of such identity-management technologies, including the possibility of morality testing, is also important given the stated purposes for extreme vetting procedures set forth in President Trump's Executive Orders on immigration. The January 27, 2017, Order specifically states that its purpose is to include an assessment of the ideological and constitutional posture of immigrants through extreme vetting:

> In order to protect Americans, the United States must ensure that those admitted to this country do not bear hostile attitudes toward it and its founding principles. The United States cannot, and should not, admit those who do not support the Constitution, or those who would place violent ideologies over American law.[256]

Although the March 6, 2017, Order does not include this language, the screening and vetting requirements set forth in section 5 are more expansive and ambiguous. For instance, instead of focusing on constitutional ideology, section 5 casts a wide precrime net, stating that the screening and vetting standards will analyze, for example, the "risk of causing harm."[257]

---

250. 562 U.S. 134 (2011).
251. 563 U.S. 582 (2011).
252. 567 U.S. 387 (2012).
253. *Nelson*, 562 U.S. at 142 (challenging whether HSPD-12 that mandates standardized credentialing for all federal employees and contractors violates a constitutional right to privacy).
254. *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*, DEP'T HOMELAND SECURITY (Aug. 19, 2015), http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm [https://perma.cc/7G8A-BEZ6].
255. *Nelson*, 562 U.S. at 138.
256. January 27, 2017, Order, *supra* note 4, § 1.
257. March 6, 2017, Order, *supra* note 8, § 5(a).

The September 24, 2017, Order increases the ambiguity of the screening and vetting mandate even further. In section 1(a) of the September 24, 2017, Order, it states that the purpose and policy of the Proclamation is "to protect its citizens from terrorist attacks and other public-safety threats. Screening and vetting protocols and procedures associated with visa adjudications and other immigration processes play a critical role in implementing that policy."[258]

The September 24, 2017, Order does not define how threat risks will be assessed, nor does it provide specific details on the "[s]creening and vetting protocols and procedures" that are prescribed. However, in several sections, including sections 1(b), 1(c)(i), and 1(d), the Order refers to the need to implement "identity-management and information-sharing protocols and procedures."[259] The opacity of these "protocols and procedures" reemphasizes the ambiguity of the precrime mandate suggested by the Orders. *Nelson*, therefore, is particularly relevant to understanding the ambition of the Orders, as the HSPD-12 program that was challenged in *Nelson* was intended to help implement "identity-management and information-sharing protocols and procedures" after the terrorist attacks of September 11, 2001.

In *Nelson*, NASA contractors argued that the background check required by the HSPD-12 program violated a constitutional right to informational privacy. The Court ruled against the NASA contractors, holding that the background-check process that was challenged consisted of "reasonable, employment-related inquiries that further the Government's interests in managing its internal operations."[260]

The Supreme Court's decision in *Nelson* was widely anticipated by privacy experts and scholars. Over three decades have passed since the Court "referred broadly to a constitutional privacy 'interest in avoiding disclosure of personal matters.'"[261] When the Court granted certiorari, therefore, some were hopeful that *Nelson* presented a ripe opportunity to reaffirm the role of a constitutional right to information privacy in safeguarding private individuals—here, privately employed scientist-contractors performing low-security-risk research for NASA through a private university—from unnecessarily overbroad disclosure requirements by the government and the risks of inadvertent or malicious exposure of personal information that could result from the government's digitalized data collection procedures. As one amicus brief filed in the case explained, "Constitutional privacy safeguards are particularly important in this case because NASA's failure to meet its

258. September 24, 2017, Order, *supra* note 13.
259. *Id.*
260. *Nelson*, 562 U.S. at 151.
261. *Id.* at 138 (quoting Whalen v. Roe, 429 U.S. 589, 599–600 (1977)); *see also* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457 (1977).

obligations under the Privacy Act and the agency's poor data security practices pose substantial risks to the scientists' personal information."[262]

Given the significance of the case, especially in light of increasing public concerns about suspicionless data mining by the government and recent well-publicized cases of database compromise through hackers, some were surprised when the Court issued its decision rather quickly and summarily, fairly soon after oral argument. In a relatively brief opinion, the Supreme Court "assume[d], without deciding, that the Constitution protects a privacy right."[263] The Court then concluded that NASA's background check, newly implemented to bring the federal agency into compliance with HSPD-12, did not violate a right to privacy, if one were to assume that such a right might exist.[264] The Court held that "[t]he Government's interests as employer and proprietor in managing its internal operations, combined with the protections against public dissemination provided by the Privacy Act of 1974, 5 U.S.C. § 552a (2006 ed. and Supp. IV), satisfy any 'interest in avoiding disclosure' that may 'arguably ha[ve] its roots in the Constitution.'"[265]

With its decision, the Supreme Court overturned a preliminary injunction that had ordered the suspension of NASA's background-check process after the Ninth Circuit found aspects of the government's questions to be in violation of the scientists' constitutional right to privacy.[266] The Supreme Court explained that the Ninth Circuit was in error because "[t]he questions challenged by respondents are part of a standard employment background check of the sort used by millions of private employers."[267] Yet, the significance of this case is misstated and misunderstood when cast as a simplistic battle over background-check protocol under the government's HSPD-12 program and whether that protocol may or may not implicate constitutional privacy interests.

Both the Supreme Court and the Ninth Circuit focused on a series of drug-related questions presumed to be the most objectionable to the scientists and that are listed on the Standard Form 85: Questionnaire for Non-Sensitive Positions ("SF 85").[268] SF 85 asks whether an employee has "used, possessed, supplied, or manufactured illegal drugs" in the last year.[269] In issuing the preliminary injunction, the Ninth Circuit concluded that the form's "'open-ended and highly private' questions . . . were not 'narrowly tailored' to meet the Government's interests in verifying contractors'

262. Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Legal Scholars and Technical Experts in Support of Respondents at 6, *Nelson*, 562 U.S. 134 (No. 09-530), 2010 WL 3167308.

263. *Nelson*, 562 U.S. at 138.

264. *Id.*

265. *Id.* (second alteration in original) (quoting *Whalen*, 429 U.S. at 599, 605).

266. Nelson v. NASA, 506 F.3d 713, 715–16 (9th Cir. 2007).

267. *Nelson*, 562 U.S. at 149.

268. *Form: SF85*, U.S. GEN. SERVICES ADMIN., https://www.gsa.gov/portal/forms/download/116378 [https://perma.cc/4JHM-6ESJ].

269. *Id.*

identities and 'ensuring the security" of the Jet Propulsion Laboratory at NASA.[270]

In a footnote, the Court noted a compelling question raised by the scientists that had been dismissed by the Ninth Circuit as unripe and had not been made the subject of a cross-petition: a question of the so-called "suitability" criteria that the government used to determine employment eligibility at Jet Propulsion Laboratory.[271] These factors include consideration of a candidate's financial and emotional health as well as things like "carnal knowledge."[272] The "suitability" criteria were derived from a ninety-four-page government vetting protocol document titled, "NASA Desk Guide for Suitability and Security Clearance Processing, Version 2."[273]

Specifically, understanding the scientists' constitutional informational privacy claim requires an understanding of the morality- and character-testing criteria that were open for questioning and evaluation during the background-check process required under NASA's implementation of HSPD-12. On page sixty-five of the desk guide, NASA includes an "Issue Characterization Chart" that allows NASA to assess individuals' character and "suitability" based on more than 100 itemized characteristics.[274] These items appeared to assess good moral character and trustworthiness. Characteristics on the evaluation include: "[d]runk"; "[b]ad check"; "[p]attern of irresponsibility as reflected in credit history"; "[c]arnal knowledge"; "indecent proposal"; "sodomy"; "voyeurism [or] peeping tom"; "[m]ailing, selling, or displaying obscene material"; "[b]eastiality"; "[p]attern of excessive [substance abuse] as reflected in inability to function responsibly [and] medical treatment or poor health"; "[d]isorderly conduct"; "[a]ttitude [and] [p]ersonality [c]onflict"; "[t]respassing"; and "[m]inor traffic violation."[275]

Upon successful completion of the NASA "Suitability and Security Clearance Processing" protocol, the desk guide authorizes the agency to issue the NASA employee or private contractor a biometric ID card in accordance with HSPD-12.[276] Failure to pass this newly implemented clearance process results in the termination of employment.[277] While the "suitability" criteria were not before the Court, the acting solicitor general nevertheless felt compelled to assert at oral argument that "NASA will not and does not use"

---

270. *Nelson*, 562 U.S. at 143.

271. *Id.* at 143 n.5.

272. *Id.*; *see also* AGENCY HUM. RES. DIV., NAT'L AERONOTICS & SPACE ADMIN., SREF-30000-0003, NASA DESK GUIDE FOR SUITABILITY AND SECURITY CLEARANCE PROCESSING VERSION 2, at 51 (2008) [hereinafter NASA DESK GUIDE], http://hspd12jpl.org/files/SuitabilitySecurityDeskGuide.pdf [https://perma.cc/957P-9PJN].

273. NASA DESK GUIDE, *supra* note 272, at 51.

274. *Id.* at 65.

275. *See Nelson*, 562 U.S. at 143 n.5; NASA DESK GUIDE, *supra* note 272, at 65–67. The NASA Desk Guide provides this caveat: "[T]raffic violations not required to be admitted on OF306 or other application material/QSP will not be considered issues." NASA DESK GUIDE, *supra* note 272, at 67.

276. NASA DESK GUIDE, *supra* note 272, at 71–93.

277. *Id.*

such objectionable criteria "to make contractor credentialing decisions."[278] The need for such assurance indicates the scientists did indeed have real privacy concerns, even if they did not crystallize into part of a live claim before the Court.

Thus, lost in this case was a real concern about what information NASA, or any other government agency, is allowed to seek under the identity-verification procedures imposed by HSPD-12 and whether the constitution, under a privacy right, imposes any fundamental limiting principles on that identity-verification process. The acting solicitor general's assurance that intimate personal details regarding credit card debt and carnal knowledge, for example, will not be considered by NASA is nothing more than that—just an assurance. Meanwhile the "suitability" criteria that could be used to determine the denial of the issuance of a biometric ID card under HSPD-12 makes clear that fears that government identity-management programs may become overbroad and overintrusive are not paranoid or baseless.

*Nelson*, by affirming HSPD-12, may now pave the way for the implementation of a biometric credentialing program and uniform biometric-based dataveillance program on a national scale. *Nelson* also demonstrates how suitable character testing or morality testing can be built into modern vetting protocols in civilian background checks, as the facts of the case demonstrated that NASA employees and contractors were required to demonstrate trustworthiness and good character before receipt of the biometric identification card.

Under a universal biometric identification system, however, suitability testing or character-vetting protocols could be embedded within the database screening system itself. Thus, the morality testing would not necessarily arrive at the front end of the vetting process, as was seen in *Nelson*. Rather, the accumulation of biometric and biographic data enables both biometric and suitability testing. Rather than clearing a suitability assessment in order to qualify for a biometric ID card, a biometric-anchored database screening system could allow for moral- and suitability-criteria testing on the back end of the vetting process. Recent disclosures by Edward Snowden, for example, explain how biometric data can be fused with biographic data to assess risk.[279]

This development in Supreme Court jurisprudence is, thus, significant because the original announcement of Trump's "Muslim Ban" indicated that the proposal was inclusive of U.S. citizens. Specifically, on December 8, 2015, shortly after then-candidate Trump announced plans for the Muslim

278. *Nelson*, 562 U.S. at 143 n.5.

279. *See* James Risen & Laura Poitras, *N.S.A. Collecting Millions of Faces from Web Images*, N.Y. TIMES (May 31, 2014), http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html [https://perma.cc/PQD8-U5DN] (explaining that biometric data can be combined with "two dozen data points" that include DHS databases and other federal databases, such as "Transportation Security Administration No Fly List, [a person's] passport and visa status, known associates or suspected terrorist ties, and comments made about [an individual] by informants to American intelligence agencies").

travel ban, he suggested in a nationally televised interview[280] that the ban could possibly extend to Muslim Americans.[281] Trump invoked former President Franklin D. Roosevelt's World War II proclamation that U.S. citizens who were potentially "enemy aliens" could be detained.[282]

On January 28, 2017, one day after President Trump signed the Executive Order imposing restrictions on the travel and immigration of citizens of Muslim-majority nations, Fox News asked former New York City Mayor Rudy Giuliani whether the Executive Order was, in fact, a Muslim ban.[283] Guiliani explained: "[W]hen [Trump] first announced it [during the campaign], he said, 'Muslim ban.' He called me up. He said, 'Put a commission together. Show me the right way to do it legally.'"[284] Giuliani elaborated further: "And what we did was, we focused on, instead of religion, *danger* . . . . Perfectly legal, perfectly sensible. And that's what the ban is based on. It's not based on religion. It's based on places where there are [sic] substantial evidence that people are sending terrorists into our country."[285] This suggests that discriminatory vetting and screening protocols can evade judicial review if a protected class is targeted indirectly through "race-neutral" criteria, such as threat risk assessments.

In *Washington v. Trump*,[286] litigation that addressed the first Executive Order, the Ninth Circuit disagreed that the government had established sufficient evidence of an impending national security threat.[287] On February 9, 2017, in upholding the Western District of Washington's grant of a temporary restraining order, halting the implementation of the Executive Order, the Ninth Circuit concluded: "[T]he Government has not offered any evidence or even an explanation of how the national security concerns that justified those designations [of travel and immigration restrictions], which triggered visa requirements, can be extrapolated to justify an urgent need for the Executive Order to be immediately reinstated."[288]

In subsequent litigation, the Fourth and Ninth Circuits agreed that the Government had failed to show a sufficient justification for the Executive Order. In *Hawaii v. Trump*,[289] the Ninth Circuit panel explained that the president had not made a "sufficient finding . . . that entry of the excluded

280. Christopher Snyder, *Trump Doubles Down on Vow to Bar Muslims*, FOX NEWS (Dec. 8, 2015), http://www.foxnews.com/politics/2015/12/08/trump-calls-for-complete-shutdown-on-muslims-entering-us.html [https://perma.cc/Q6ZF-8F96].

281. *See* Ali Vitali, *At South Carolina Rally, Donald Trump Defiant on Muslim Ban*, NBC NEWS (Dec. 7, 2015), http://www.nbcnews.com/politics/2016-election/south-carolina-rally-trump-defiant-steadfast-muslim-ban-n475951 [https://perma.cc/D3WC-5S56].

282. Snyder, *supra* note 280.

283. Amy B. Wang, *Trump Asked for a 'Muslim Ban,' Giuliani Says—and Ordered a Commission to Do It 'Legally,'* WASH. POST (Jan. 29, 2017), https://www.washingtonpost.com/news/the-fix/wp/2017/01/29/trump-asked-for-a-muslim-ban-giuliani-says-and-ordered-a-commission-to-do-it-legally/ [https://perma.cc/G7YY-JG5A].

284. *Id.*

285. *Id.*

286. 847 F.3d 1151 (9th Cir. 2017) (per curiam).

287. *Id.* at 1168.

288. *Id.* at 1168 n.7.

289. 859 F.3d 741 (9th Cir.) (per curiam), *cert. granted*, 137 S. Ct. 2080 (2017).

classes would be detrimental to . . . the United States."[290] In *International Refugee Assistance Project*, the Fourth Circuit noted that while the government argued that it had a national security purpose in issuing the Order, evidence supporting such a purpose was "comparably weak[er]" than then-candidate Trump's statements about a Muslim ban, subsequent statements on the issues, statements made by his advisors, as well as the issuance of and statements made by President Trump and his advisors regarding the second Executive Order.[291] At the time this Article was written, the Supreme Court had granted certiorari in both cases and consolidated them for argument.[292]

On February 24, 2017, the Associated Press reported that a leaked memo drafted at the request of the DHS acting Under Secretary for Intelligence and Analysis concluded "citizenship is an unlikely indicator of terrorism threats to the United States."[293] The memo states that the analysis undertaken by DHS specifically analyzed the threat of the "seven countries [that were] impacted by [section 3 of Executive Order] 13769."[294] The DHS memo states that "of [eighty-two] people the government determined were inspired by a foreign terrorist group to carry out or try to carry out an attack in the United States [since the Syrian conflict commenced in March 2011], just over half were U.S. citizens born in the United States."[295] The DHS memo further states that the terrorists were from "[twenty-six] countries, led by Pakistan, Somalia, Bangladesh, Cuba, Ethiopia, Iraq and Uzbekistan. Of these, only Somalia and Iraq were among the seven nations included in the ban."[296] Both the Ninth and Fourth Circuits discussed this memorandum and relied on it in their rulings.[297]

Importantly, the original January 27, 2017, Order states that vetting policy should include a test to assess fidelity to founding principles and the Constitution.[298] Statements by Trump suggest that such vetting should

290. *Id.* at 770, 775.

291. Int'l Refugee Assistance Project v. Trump, 857 F.3d 554, 591–92 (4th Cir.), *cert. granted*, 137 S. Ct. 2080 (2017) ("Plaintiffs also point to the comparably weak evidence that EO-2 is meant to address national security interests, including the exclusion of national security agencies from the decision-making process, the post hoc nature of the national security rationale, and evidence from DHS that EO-2 would not operate to diminish the threat of potential terrorist activity.").

292. Trump v. Int'l Refugee Assistance Project, 137 S. Ct. 2080, 2086 (2017). The author reserves for future scholarship further inquiry into and analysis of the Supreme Court's final disposition and resolution of these matters.

293. Vivian Salama & Alicia A. Caldwell, *DHS Report Disputes Threat from Banned Nations*, ASSOCIATED PRESS (Feb. 24, 2017), http://bigstory.ap.org/article/39f1f8e4ceed4a30a4570f693291c866/dhs-intel-report-disputes-threat-posed-travel-ban-nations [https://perma.cc/Z8NL-8VW6].

294. Memorandum from the Dep't of Homeland Sec., Office of Intelligence and Analysis, Citizenship Likely an Unreliable Indicator of Terrorist Threat to the United States (2017), https://fas.org/irp/eprint/dhs-7countries.pdf [https://perma.cc/GKK4-TVG4].

295. Salama & Caldwell, *supra* note 293.

296. *Id.*

297. Hawaii v. Trump, 859 F.3d 741, 759, 784 n.23 (9th Cir.) (per curiam), *cert. granted*, 137 S. Ct. 2080 (2017); Int'l Refugee Assistance Project v. Trump, 857 F.3d 554, 575, 591–92, 596 (4th Cir.), *cert. granted sub nom.* 137 S. Ct. 2080 (2017).

298. January 27, 2017, Order, *supra* note 4, § 1.

include a test to assess loyalty to the United States and whether an individual will "support our country, and love deeply our people."[299] He further promoted, as a candidate, the implementation of profiling and preventative measures, such as mass surveillance, to assess terroristic risk.[300]

In *Nelson*, twin innovations in national security policy and biometric surveillance policy included a machine-readable biometric ID card encoded with digitalized biometric data and other personally identifiable data, as was required by the HSPD-12 program. In the suitability criteria developed by NASA, a version of extreme vetting emerged. The January 27, 2017, Order discusses the need to implement loyalty tests that demonstrate "pro-American" values. Thus, extreme vetting may be expanded to encompass similar abstract assessments of character and morality as a part of threat risk assessments.

By affirming the credentialing protocol surrounding HSPD-12 and sanctioning an identity-management technology, *Nelson* opens the door to profound questions of constitutional law, electronic privacy law and policy, and surveillance policy that have yet to be resolved. These questions include the role of biometric technology and dataveillance in national security policy and immigration-control policy. It now remains to be seen whether HSPD-12 will eventually serve as a programmatic and technological prototype for a national biometric ID system, such as a biometric social security card or biometric ePassport, in the future.

### *B. Delegating Vetting and Database Screening Protocols to States and Private Entities*

In addition to de facto discrimination, Algorithmic Jim Crow regimes can promote de jure discrimination or discrimination as a matter of law.[301] Under historic Jim Crow regimes, enforcement of segregationist laws was delegated to both public and private entities.[302] Those who participated in segregation gatekeeping often did so under the threat of legally imposed sanctions.[303]

Resistance to the mandate to segregate train service, for instance, led to the initiation of a legal challenge to Louisiana's Jim Crow laws in *Plessy*, which required the cooperation of railway companies that were frustrated with their

299. Michael D. Shear & Helene Cooper, *Trump Bars Refugees and Citizens of 7 Muslim Countries*, N.Y. TIMES (Jan. 27, 2017), www.nytimes.com/2017/01/27/us/politics/trump-syrian-refugees.html [https://perma.cc/6UDJ-QCMR].

300. *See* Schultheis, *supra* note 99.

301. *See* Mack, *Law, Society, Identity*, *supra* note 104, at 394–95 (observing that de jure discrimination reflected both a shift in law and social rhetoric).

302. *See generally* Sunstein, *supra* note 232.

303. *See* David Benjamin Oppenheimer, *Martin Luther King,* Walker v. City of Birmingham*, and the Letter from Birmingham Jail*, 26 U.C. DAVIS L. REV. 791, 796 (1993) ("[S]hortly before King's arrival the bus station manager had been jailed for permitting African American passengers to use the white waiting room."); *see also* TOM R. TYLER, WHY PEOPLE OBEY THE LAW 21 (1990) ("Social control refers specifically to altering citizens' behavior by manipulating access to valued social resources or by delivering or threatening to deliver sanctions.").

gatekeeping duties under the Separate Car Act.[304] Railway companies opposed the segregation law on the ground that running two train cars—one for white passengers and one for black passengers—was economically costly, especially for train routes on which ridership had proven to be light.[305] The petitioners also argued that it was unlawful to delegate segregationist gatekeeping to the private companies who would be fined for allowing black passengers to ride white railcars.[306] Homer Adolph Plessy had been selected to violate the Jim Crow law specifically because he was a light-skinned black man who could "pass" as a white man.[307]

Yet, a similar de jure discrimination scheme may be emerging in the modern era. How do private and state immigration gatekeepers determine whether an individual is lawfully present in the United States? Under the Immigration Reform and Control Act of 1986 (IRCA),[308] the federal government delegated immigration enforcement authority to all employers, public and private, to assist in immigration gatekeeping duties through the examination of paper-based documents that purport to establish identity and citizenship status.[309] Under IRCA, employers faced civil and criminal fines for failure to participate in sorting out undocumented immigrants from the workforce.[310]

In 1990, the *Wall Street Journal* editorial pages compared federal employer-sanctioning policies required under federal immigration law to historic Jim Crow regimes. The publication explained that private entities were once again asked to engage in discrimination[311] under the law by effectually being deputized as immigration gatekeepers. Specifically, the *Wall Street Journal* described IRCA as "the first legislation since Jim Crow where the government is so closely aligned with a process that produces discrimination."[312]

From the 1970s to the present, immigration laws at the federal and state level have attempted to restrict immigrant access to transportation and travel, employment, education, housing, and benefits.[313] In contrast to historic Jim

304. Harris, *supra* note 105, at 187, 207 (citing 1890 La. Acts 111).

305. HIGGINBOTHAM, *supra* note 105, at 88.

306. Harris, *supra* note 105, at 212–13.

307. *Id.* at 212.

308. Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, 100 Stat. 3359 (codified in scattered sections of 8 U.S.C.).

309. *See* 8 U.S.C. §§ 1324a (2012).

310. *Id.*

311. Studies by the U.S. Government Accountability Office found that the employer sanctions provision of the Immigration Reform and Control Act of 1986 had resulted in widespread discrimination. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO/T-GGD-92-21, IRCA-RELATED DISCRIMINATION: ACTIONS HAVE BEEN TAKEN TO ADDRESS IRCA-RELATED DISCRIMINATION, BUT MORE IS NEEDED 2 (1992), http://www.gao.gov/products/T-GGD-92-21 [https://perma.cc/9UV4-7M45]; U.S. GOV'T ACCOUNTABILITY OFFICE, GAO/T-GGD-90-51, IRCA ANTI-DISCRIMINATION AMENDMENTS OF 1990, at 3 (1990), http://www.gao.gov/products/T-GGD-90-51 [https://perma.cc/CU9N-8LYS].

312. Editorial, *Clocking Immigration Sanctions*, WALL ST. J., Apr. 16, 1990, at A12.

313. *See* Motomura, *supra* note 62, at 1361; Michael J. Wishnie, *Laboratories of Bigotry?: Devolution of the Immigration Power, Equal Protection, and Federalism*, 76 N.Y.U. L. REV. 493, 513–14 & nn.106–10 (2001); *see also* Stephen Lee, *Private Immigration Screening in the*

Crow regimes, however, the targeting of the undocumented immigrant population does not need to proceed under a façade of "equality" because such discrimination is often construed as legally permissible. Undocumented immigrants, with important exceptions, do not enjoy the broad civil rights protections and constitutional rights afforded to U.S. citizens.[314] Even lawful immigrants may face more restricted rights than U.S. citizens.[315] Those arguing in favor of tough immigration actions, including those defending the Executive Orders, have explained this position as a legal defense of such actions.[316]

Yet, for decades, lawful immigrants and those perceived to be foreign have alleged that they suffer from a form of collateral discrimination: an assumption of undocumented status and accidental targeting that stems from restrictive immigration laws.[317] Studies have consistently shown that vetting and screening protocols required by immigration gatekeeping—sometimes referred to as "show me your papers" laws—incentivize racial profiling.[318] In other words, mandatory document checks often target those perceived to be foreign: those who may be isolated on the basis of race, color, ethnicity, national origin, religion, and "foreignness" characteristics,[319] such as accent, clothing, and a failure to present "whiteness" characteristics.[320]

In response to growing empirical evidence that immigration-related screening and delegated gatekeeping duties by the government reliably led to discrimination, Congress increasingly looked to technological screening methods as "race-neutral" tools to achieve the same means.[321] Throughout the 1990s until the present, immigration reform legislation has proposed database-driven methods to implement screening and gatekeeping

*Workplace*, 61 STAN. L. REV. 1103, 1130 (2009); Huyen Pham, *The Private Enforcement of Immigration Laws*, 96 GEO. L.J. 777, 780–81 (2008).

314. *See* Hiroshi Motomura, *The Curious Evolution of Immigration Law: Procedural Surrogates for Substantive Constitutional Rights*, 92 COLUM. L. REV. 1625, 1632 (1992). The Supreme Court has recognized potential due process claims of persons in the United States who are noncitizens including those present unlawfully. *See* Kerry v. Din, 135 S. Ct. 2128, 2133–34 (2015); Zadvydas v. Davis, 533 U.S. 678, 692–95 (2001); Landon v. Plasencia, 459 U.S. 21, 33–34 (1982); Kleindienst v. Mandel, 408 U.S. 753, 762–65 (1972).

315. *See* 8 U.S.C. § 1324b(a)(3)(B) (2012) (restricting certain protections under the antidiscrimination provision of the Immigration and Nationality Act to those immigrants with lawful permanent residence status).

316. Reply in Support of Emergency Motion for Stay Pending Appeal at 5, Washington v. Trump, 847 F.3d 1151 (9th Cir. 2017) (per curiam) (No. 17-35105), 2017 WL 492504.

317. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO/T-GGD-90-51, IRCA ANTI-DISCRIMINATION AMENDMENTS OF 1990, *supra* note 311, at 3.

318. *Id.*

319. *Id.*

320. *Id.*; *see also* Cheryl I. Harris, *Whiteness as Property*, 106 HARV. L. REV. 1707, 1725 (1993).

321. *See* Basic Pilot Program Extension and Expansion Act of 2003, Pub. L. No. 108-156, 117 Stat. 1944 (codified at 8 U.S.C. §§ 1101, 1324a (2012)) (authorizing the development of the "basic pilot program for employment eligibility verification" to implement a technologically improved method to screen immigrants).

functions.[322] Many of these database screening methods are experimental and still under testing.[323]

Nonetheless, the 9/11 terror attacks accelerated the rollout of these experimental vetting and screening systems.[324] The immigrant status of the 9/11 hijackers led to calls for policy initiatives that could facilitate the identification and more efficient tracking of immigrants and potential terrorists through cybersurveillance and dataveillance technologies.[325] Many of these technologies were dependent upon biometric data monitoring and database-facilitated algorithmic sorting tools.[326] The impetus was not so much to avoid bias in screening but to harness the supposed efficiencies and reliability of a database-centered means of screening.

Since 9/11, immigration policy and national security policy have increasingly converged. At the federal level, this convergence could be seen in the increasing adoption of big data identity-management systems aimed to screen the population to determine who could receive rights and benefits, such as the No Fly List,[327] the No Work List ("E-Verify"),[328] and the No

322. *See id.*

323. *Id.* § 3(b)(b)(1) ("[E]valuating whether the problems identified by the report submitted under subsection (a) have been substantially resolved . . . ."); *id.* § 3(b)(b)(2) ("[D]escribing what actions the Secretary of Homeland Security shall take before undertaking the expansion of the basic pilot program to all 50 States in accordance with section 401(c)(1), in order to resolve any outstanding problems raised in the report filed under subsection (a).").

324. *See* Press Release, Transp. Sec. Admin., TSA to Test New Passenger Pre-Screening System (Aug. 26, 2004), http://www.tsa.gov/press/releases/2004/08/26/tsa-test-new-passenger-pre-screening-system [https://perma.cc/8RRW-8L9P] (describing the implementation of a post-9/11 passenger prescreening program that checks passengers' names against terrorist watchlists in an effort to improve the use of "no fly" lists).

325. The 9/11 Commission Report, for example, emphasized the need to incorporate biometric data into identity-management tools and systems in order to augment border security and national security objectives. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 385–92 (2004), http://www.9-11commission.gov/report/911Report.pdf [https://perma.cc/RT32-JKEZ] ("Linking biometric passports to good data systems and decision-making is a fundamental goal.").

326. *See* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 37–67 (2000); KELLY A. GATES, OUR BIOMETRIC FUTURE: FACIAL RECOGNITION TECHNOLOGY AND THE CULTURE OF SURVEILLANCE 1–2 (2011) ("The suggestion that an automated facial recognition system may have helped avert the September 11 terrorist attacks was perhaps the most ambitious claim circulating about biometric identification technologies in the aftermath of the catastrophe."); ANIL K. JAIN ET AL., INTRODUCTION TO BIOMETRICS vii (2011) ("[T]he deployment of biometric systems has been gaining momentum over the last two decades in both public and private sectors. These developments have been fueled in part by recent [post-9/11] government mandates stipulating the use of biometrics for ensuring reliable delivery of various services."). *See generally* JENNIFER LYNCH, FROM FINGERPRINTS TO DNA: BIOMETRIC DATA COLLECTION IN U.S. IMMIGRANT COMMUNITIES AND BEYOND (2012); Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407 (2012); Hu, *supra* note 52.

327. 49 U.S.C. § 44903 (2012); 49 C.F.R. pts. 1540, 1544, 1560 (2016).

328. E-Verify is a "test pilot" program jointly operated by DHS and the Social Security Administration that enables employers to screen employees' personally identifiable data (e.g., name, birth date, and Social Security number) through government databases over the internet in order to "verify" the identity of the employee. U.S. CITIZENSHIP & IMMIGR. SERVS., DEP'T OF HOMELAND SEC., E-VERIFY USER MANUAL FOR EMPLOYERS 1 (2014), http://www.uscis.gov/sites/default/files/files/nativedocuments/E-Verify_Manual.pdf

Citizenship List (managed by Secure Communities[329] and the DHS's Prioritized Enforcement Program[330]). These database screening and digital watchlisting systems purport to further crime control, immigration control, and counterterrorism objectives. The E-Verify database has not only been used to restrict employment opportunities, but it is alleged that landlords have used the database to screen tenants and that school officials have used the database to screen students.[331] Similarly, the No Vote List ("SAVE"[332] and

---

[https://perma.cc/DB3D-P3MQ]. 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; *see also* Basic Pilot Program Extension and Expansion Act of 2003, Pub. L. No. 108-156, 117 Stat. 1944 (codified at 8 U.S.C. §§ 1101, 1324a (2012)); Basic Pilot Extension Act of 2001, Pub. L. No. 107-128, 115 Stat. 2407 (2002) (codified at 8 U.S.C. §§ 1101, 1324a). For a thorough discussion of E-Verify and its legal implications, see generally Juliet P. Stumpf, *Getting to Work: Why Nobody Cares About E-Verify (And Why They Should)*, 2 U.C. IRVINE L. REV. 381 (2012).

329. Secure Communities ("S-COMM") is an interoperability program that facilitates data sharing and database screening protocols between the FBI, DHS, and local law enforcement agencies. 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). *See generally* Adam B. Cox & Thomas J. Miles, *Policing Immigration*, 80 U. CHI. L. REV. 87 (2013); Christopher N. Lasch, *Rendition Resistance*, 92 N.C. L. REV. 149 (2013); Thomas J. Miles & Adam B. Cox, *Does Immigration Enforcement Reduce Crime? Evidence from Secure Communities*, 57 J.L. & ECON. 937 (2014). 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. Immigr. & Customs Enf't, U.S. Dep't of Homeland Sec. (Oct. 2, 2010), http://uncoverthetruth.org/wp-content/uploads/2012/01/Mandatory-in-2013-Memo.pdf [https://perma.cc/CW98-2Y9G]. The authorities relied upon by DHS include: (1) 28 U.S.C. § 534(a)(1) and (4), which provides the FBI with authority to share fingerprint data with ICE; (2) 8 U.S.C. § 1722, which 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) 42 U.S.C. § 14616, which ratifies information or database sharing between federal and state agencies. *Id.* at 4–6.

330. The DHS Prioritized Enforcement Program (PEP) was announced by DHS Secretary Jeh Johnson 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 Director, Immigr. & Customs Enf't 2 (Nov. 20, 2014), http://www.dhs.gov/sites/default/files/publications/14_1120_memo_secure_communities.pdf [https://perma.cc/SCL3-Z7YX]. On February 20, 2017, former DHS Secretary John Kelly signed an implementation memo announcing that S-COMM would be reinstated and PEP would be rescinded. *See* Memorandum from John Kelly, Sec'y of Homeland Sec., to Kevin McAleenan, Acting Comm'r, U.S. Customs & Border Prot., Enforcement of the Immigration Laws to Serve the National Interest (Feb. 20, 2017), https://www.dhs.gov/sites/default/files/publications/17_0220_S1_Enforcement-of-the-Immigration-Laws-to-Serve-the-National-Interest.pdf [https://perma.cc/7SJE-9RS2].

331. Stumpf, *supra* note 328, at 400 n.87 (citing MARC R. ROSENBLUM, EVERIFY: STRENGTHS, WEAKNESSES, AND PROPOSALS FOR REFORM, MIGRATION POL'Y INST. 5, 7 (2011); Mary D. Fan, *Post-Racial Proxies: Resurgent State and Local Anti-"Alien" Laws and Unity-Rebuilding Frames for Antidiscrimination Values*, 32 CARDOZO L. REV. 905, 923–24, 935–36 (2011); Kati L. Griffith, *Discovering 'Immployment' Law: The Constitutionality of Subfederal Immigration Regulation at Work*, 29 YALE L. & POL'Y REV. 389, 417, 424–26 (2011); Rigel C. Oliveri, *Between a Rock and a Hard Place: Landlords, Latinos, Anti-Illegal Immigrant Ordinances, and Housing Discrimination*, 62 VAND. L. REV. 55, 116 (2009)).

332. In recent years, state election officials have used the Systematic Alien Verification for Entitlements (SAVE) database screening protocol to conduct voter purges. *See* Fatma Marouf,

"HAVA"[333]) has been used for voter purges and to restrict driver's licenses as well as access to welfare benefits.[334]

After 9/11, the federal government sought a sharp increase in personnel who could conduct vetting and implement screening protocols to increase the effectiveness of immigration gatekeeping.[335] Thus, the federal government also increasingly invited state and local law enforcement to participate in the enforcement of federal immigration law under a "force multiplier" theory[336] of delegation of immigration gatekeeping.[337] Under the expanded immigration gatekeeping mandates of DHS, state and local governments were granted access to DHS database screening systems and invited to screen arrestees through these systems.[338] After 9/11, the federal government also experimented with the merging of database screening protocols to eliminate the separation between civil and criminal immigration database screening protocols.[339]

Under immigration federalism and national security federalism, state laws have increasingly captured post-9/11 identity-management technologies introduced by DHS. Consequently, comparisons between historic Jim Crow regimes and contemporary immigration enforcement regimes have intensified in recent years. De jure discrimination has been alleged in state laws that mandate vetting protocols and the delegation of vetting and

---

*The Hunt for Noncitizen Voters*, 65 STAN. L. REV. ONLINE 66, 66 (2012). For more information on the SAVE database screening program, see DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS (SAVE) PROGRAM 12 (Aug. 26, 2011), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_save.pdf [https://perma.cc/7976-2BYA].

333. 52 U.S.C. § 21083 (2012) (originally enacted as Help America Vote Act of 2002 (HAVA), Pub. L. No. 107-252, 116 Stat. 1666 (2002)). HAVA requires each state to implement and maintain an electronic database of all registered voters. *Id.* 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.* § 21083(a)(5)(A)(i). If the individual has neither number, the state is required to assign a voter identification number to the applicant. *Id.* § 21083(a)(5)(A)(ii). Each state election office is tasked with overseeing 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 [https://perma.cc/5TFK-M4MM].

334. *See SAVE Database—Issues with Obtaining SSN and Driver's Licenses*, NAFSA, http://www.nafsa.org/findresources/Default.aspx?id=11154 [https://perma.cc/3ZPW-TDFZ] (last visited Oct. 16, 2017).

335. *See* Jennifer M. Chacón, *The Transformation of Immigration Federalism*, 21 WM. & MARY BILL RTS. J. 577, 589 (2012); Kobach, *supra* note 63, at 545; Christopher N. Lasch, *Preempting Immigration Detainer Enforcement Under* Arizona v. United States, 3 WAKE FOREST J.L. & POL'Y 281, 328 (2013).

336. *See* Memorandum from John Kelly, Sec'y of Homeland Sec., to Kevin McAleenan, Acting Comm'r, U.S. Customs and Border Prot. et al., Implementing the President's Border Security and Immigration Enforcement Improvements Policies 4 (Feb. 20, 2017), https://www.dhs.gov/sites/default/files/publications/17_0220_S1_Implementing-the-Presidents-Border-Security-Immigration-Enforcement-Improvement-Policies.pdf [https://perma.cc/RX6G-GBTM].

337. *Id.*

338. *See supra* note 329 and accompanying text.

339. S-COMM involves both civil DHS immigration database screening and FBI criminal record database screening simultaneously. *See supra* note 329 and accompanying text.

screening responsibilities. Similar to the segregationist gatekeeping duties that were delegated under historic Jim Crow regimes, restrictionist immigration gatekeeping protocols under Algorithmic Jim Crow have been criticized as promoting both de jure and de facto discrimination against citizens and lawful immigrants that may be perceived to be foreign.[340] Specifically, state laws have proposed that legal penalties and liabilities could be incurred by employers, police, landlords, doctors, school officials, and state benefits administrators who fail to conduct vetting and screening protocols.

For instance, the *Los Angeles Times* invoked Jim Crow comparisons after passage of Alabama House Bill 56, a state law that attempted to control unwanted migration in part by delegating immigration screening to both private and public entities.[341] Wade Henderson, president of the Leadership Conference on Civil and Human Rights, also drew a comparison. On June 9, 2011, the day Alabama House Bill 56 was signed into law, he remarked: "[E]ven Bull Connor himself would be impressed," referring to the famed segregationist who served as Birmingham's public safety commissioner tasked with enforcing the city's Jim Crow laws during the 1950s.[342]

Similarly, the governor of Arizona signed SB 1070 into law in 2013, referred to as the "racial profiling" law and the "show me your papers law."[343] Shortly thereafter, Reverend Lennox Yearwood of the Hip Hop Caucus, wearing a "Boycott Arizona" cap, declared during an interview that the Arizona immigration law is "our Jim Crow moment for the 21st century."[344] He further stated, "We can't have anyone being checked based on the hue of their color . . . . We need to put our lives on the line [in protest] . . . . We need to stand up."[345] Members of Congress likened the Arizona law to Jim Crow and historic apartheid systems.[346]

In future comprehensive immigration reform proposals and in the implementation of extreme vetting protocols—especially with the Supreme Court in both *Whiting* and *Arizona* apparently endorsing a potential merger between criminal and civil database screening protocols—it is possible that

340. *See, e.g.*, Kevin R. Johnson, *A Case Study of Color-Blindness: The Racially Disparate Impacts of Arizona's S.B. 1070 and the Failure of Comprehensive Immigration Reform*, 2 U.C. IRVINE L. REV. 313, 319–20 (2012); Karla Mari McKanders, *Immigration Enforcement and the Fugitive Slave Acts: Exploring Their Similarities*, 61 CATH. U. L. REV. 921, 947 (2012).

341. Beason-Hammon Taxpayer and Citizen Protection Act, No. 2011-535 (2011) (codified at ALA. CODE §§ 31-13-1 to 31-13-30, 32-6-9 (2017)).

342. Richard Fausset, *Alabama Enacts Anti-Illegal-Immigration Law Described As Nation's Strictest*, L.A. TIMES (June 10, 2011), http://articles.latimes.com/2011/jun/10/nation/la-na-alabama-immigration-20110610 [https://perma.cc/3Y6E-4Y3B] ("'This draconian initiative signed into law this morning by Gov. Robert Bentley is so oppressive that even Bull Connor himself would be impressed,' said Wade Henderson, head of the Leadership Conference on Civil and Human Rights . . . . 'HB 56 is designed to do nothing more than terrorize the state's Latino community.'").

343. Kasie Hunt, *Dems: Ariz Law Like Jim Crow, Apartheid*, POLITICO (Apr. 28, 2010), http://www.politico.com/news/stories/0410/36503.html [https://perma.cc/6E8S-SW6E].

344. Michael McIntee, *AZ Is Our Jim Crow Moment of 21st Century*, YOUTUBE (July 24, 2010), http://www.youtube.com/watch?v=sAbTzyegrDU [https://perma.cc/L2MR-TKDZ].

345. *Id.*

346. Hunt, *supra* note 343.

other public and private actors could be delegated counterterrorism intelligence-gathering duties pursuant to immigration gatekeeping duties under the "force multiplier" approach. In *Whiting*, the Supreme Court upheld the constitutionality of delegating immigration database screening to private employers through the passage of the Legal Arizona Workers Act (LAWA).[347] Under LAWA, employers in Arizona were not only document-inspecting immigration gatekeepers.[348] LAWA also transformed public and private employers into database screening gatekeepers through a legal requirement that they run all new hires through the E-Verify identity-management system, which allows employers to screen employees through various federal agency databases.[349]

Similarly, in *Arizona*, the Supreme Court upheld the constitutionality of delegating immigration-database screening to state and local law enforcement after the passage of Arizona's SB 1070.[350] Similar to LAWA, state and local law enforcement were transformed into database screening gatekeepers through a legal requirement that they run all arrestees and those suspected of unlawful presence through S-COMM, an internet-based database screening system that checks biometric data (scanned fingerprints) against DHS and FBI databases.

For example, in addition to Arizona's establishment of an employer-sanctioning regime in LAWA (holding private employers responsible), and a police-sanctioning regime in SB 1070 (holding state and local law enforcement responsible), the state proposed a landlord-sanctioning regime in SB 1611,[351] enacted a state-worker-sanctioning regime in HB 2008,[352] proposed a hospital-worker-sanctioning regime in SB 1405,[353] and proposed and enacted a public-school-worker- or teacher-sanctioning regime in SB 1407[354] and SB 1141.[355]

Each of Arizona's proposed sanctioning regimes requires a screening or vetting system because otherwise, the Arizona legislature has contended, it

---

347. *See* Legal Arizona Workers Act, ch. 279, 2007 Ariz. Sess. Laws 1312 (codified at ARIZ. REV. STAT. ANN. §§ 13-2009, 23-211 to 23-214 (2008)).

348. Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, 100 Stat. 3359 (codified in scattered sections of 8 U.S.C.).

349. *See supra* note 328 and accompanying text.

350. Arizona v. United States, 567 U.S. 387, 416 (2012). Section 2(B) of SB 1070, which was slightly modified and later codified in the Arizona Revised Statutes, provides:

> For any lawful stop, detention or arrest made by [an Arizona] law enforcement official or a law enforcement agency . . . in the enforcement of any other law or ordinance of a county, city or town or this state where reasonable suspicion exists that the person is an alien and is unlawfully present in the United States, a reasonable attempt shall be made, when practicable, to determine the immigration status of the person, except if the determination may hinder or obstruct an investigation. Any person who is arrested shall have the person's immigration status determined before the person is released.

ARIZ. REV. STAT. ANN. § 11-1051 (2012).

351. S.B. 1611, 50th Leg., 1st Reg. Sess. (Ariz. 2011).

352. ARIZ. REV. STAT. ANN. §§ 1–501, 1–502 (Supp. 2011).

353. S.B. 1405, 50th Leg., 1st Reg. Sess. (Ariz. 2011).

354. S.B. 1407, 50th Leg., 1st Reg. Sess. (Ariz. 2011).

355. ARIZ. REV. STAT. ANN. § 15–802 (Supp. 2011).

could not verify who among its residents is an unauthorized immigrant and who is not. The identity-management technology often relied upon by the state gatekeeping law involved an algorithm-based database screening protocol, often supplemented by a paper-based inspection, to log personally identifiable data into a preexisting vetting and database screening system operated by DHS. Although not all of these measures passed, the gatekeeping and screening aspects of Arizona's proposed comprehensive immigration reform strategy, as well as other state and local laws passed or considered in recent years, has resulted in an unprecedented expansion of document inspection and database-driven screening protocols.[356]

Arizona's aggressive stance on restrictive immigration gatekeeping is enabled by the introduction of big data vetting analytics and database screening potentialities, often conducted through internet-based screening of DHS and other federal agency databases. It shows the multifold opportunities for electronic vetting in daily life. And while it is a system to screen out immigrants, at the national level and in the national security context, newly emerging digital watchlisting and database screening programs such as the No Fly List make clear that database screening is easily adaptable to other kinds of vetting for various purposes. Those screened or vetted will individually encounter a purportedly neutral and colorblind process but with the result that they fall into groups that can start to look much like the kinds of classifications that would normally offend the Constitution's equal protection guarantees.

Consequently, the extreme vetting protocols and the implementation of a Muslim registry should be understood within the context of delegated database screening protocols, such as those proposed and passed by Arizona. As can be seen in the discussion above, the efforts by the federal and state government to collect and screen data under the auspices of immigration-control policy now extend to a wide range of contexts, including employment screening and day-to-day policing. This appears to be consistent with data-collection and screening policies under the Trump administration. "Asked where [Muslims] would be registered, [Trump] said Muslims would be signed up at 'different places . . . . [I]t's all about [data] management.'"[357] Candidate Trump specifically referred to the need to deploy DHS identity-management technologies: "Trump tied his reasoning for the database to the need to identify who is in the country legally. 'It would stop people from coming in illegally,' Trump said. 'We have to stop people from coming into our country illegally.'"[358]

356. *See* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R-C.L.L. REV. 435, 439–40 (2008).

357. Vaughn Hillyard, *Donald Trump's Plan for a Muslim Database Draws Comparison to Nazi Germany*, NBC NEWS (Nov. 20, 2015), http://www.nbcnews.com/politics/2016-election/trump-says-he-would-certainly-implement-muslim-database-n466716 [https://perma.cc/RML4-KTZK].

358. *Id.*

### *C. Litigating Algorithmic Jim Crow*

The number of individuals and private entities affected by government identity-management programs is growing as rapidly as the programs themselves, and future attempts to seek judicially imposed limits on such programs appear inevitable. The broader question, thus, is not whether the scientists in *Nelson* were denied a constitutional right to privacy but whether any limiting principle can be articulated to curtail the government's attempt to engage in post-9/11, semiuniversal vetting and screening systems, such as the No Fly List, and biometric dataveillance credentialing, such as HSPD-12, in the name of furthering national security, crime control, and immigration policy.

Under an "equal but separate" regime, identity-management systems that purport to collect and sort data of individuals equally, however, may impose disparate consequences through colorblind vetting protocols and "race-neutral" database screening systems. Yet, whether biometric-based identification systems can be presented as colorblind and "race-neutral" is in doubt. Racial characteristics are among the data collected in biometric databases. Soft biometric data, for instance, includes digital analysis or automated determination of age, height, weight, race or ethnicity, color of skin and color of hair, scars and birthmarks, and tattoos.[359] Further, newly developed big data vetting tools fuse biometric data with biographic data and internet and social media profiling to algorithmically assess risk. Data fusion techniques are not race neutral, as recent reports have exposed how data analytics can result in pinpointing racial, ethnic, and socioeconomic characteristics through big data analysis tools.[360] As plaintiffs in the No Fly List litigation allege, those disparately impacted by mandatory vetting and screening protocols will largely fall within traditional classifications—race, color, national origin, ethnicity, and religion—depending on what may be determined to be suspect criteria.[361]

Recent immigration-control policy and programs demonstrate the government's interest in delegating immigration-vetting duties to private actors,[362] such as employers, and nonfederal actors, such as state and local law enforcement[363] or their privatized subdelegates,[364] which can exacerbate issues of racial profiling and discrimination. For instance, LAWA and Arizona's SB 1070 are examples of immigration federalism and national security federalism. Immigration federalism traditionally has denoted state

359. ENCYCLOPEDIA OF BIOMETRICS 1235 (Stan Z. Li & Anil K. Jain eds., 2009).

360. *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 56 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/G4WC-7NN6].

361. *See* Complaint at 8–9, Latif v. Holder, 28 F. Supp. 3d 1134 (D. Or. 2014) (No. 10-CV-750-BR).

362. *See* Lee, *supra* note 313, at 1130; Pham, *supra* note 313, at 780–81; Stumpf, *supra* note 328, at 382.

363. *See generally* Cox & Miles, *supra* note 329; Lasch, *supra* note 329.

364. *See* Jennifer M. Chacón, *Privatized Immigration Enforcement*, 52 HARV. C.R-C.L.L. REV. 1, 8 (2017).

and local efforts to control or mitigate the impact of unwanted migration or to regulate the admission of noncitizens across state borders.[365] In the past few years, several thousand state and local immigration-related laws have been considered in almost every state.[366] This level of immigration federalism activity is unprecedented in U.S. history.[367]

Also unprecedented, however, is the manner in which immigration federalism is intersecting with two other critical movements in U.S. history: (1) an increasing reliance on database-sorting technology and dataveillance in federal immigration policy to facilitate state-federal partnerships in the control of unwanted migration; and (2) a post-9/11 national security policy of national security federalism that encourages a state-federal partnership in the furtherance of intelligence-gathering and homeland security objectives under a "force multiplier" theory.

In the DHS memos released by then-DHS Secretary John Kelly on February 21, 2017, which implemented the Executive Orders on immigration signed by President Trump on January 25, 2017, DHS stated that the executive branch would apply a "force multiplier" approach to the immigration-control and national security effort.[368] Identity-management technologies that rely upon the internet and digital databases to verify identity have been developed to help execute these goals. As a presidential candidate, Trump explained that immigration-control and counterterrorism efforts required "a lot of systems, beyond databases."[369]

Because these statutes are perceived as targeting primarily those born in foreign countries but residing here, the questions of government intrusion and disparate impact are obscured. However, while the state and federal laws at issue may be immigration laws first, they are still identity-screening laws, and the entire population—citizens and noncitizens—is subject to their vetting and screening protocols. Consequently, immigration federalism, when combined with national security federalism, is driving the exponential expansion of identity-management programs and biometric-database screening.

Given the historical connection between mass data collection and mass discrimination,[370] federal courts may require an inquiry into the

365. *See* Hiroshi Motomura, *The Rights of Others: Legal Claims and Immigration Outside the Law*, 59 DUKE L.J. 1723, 1729 (2010) ("Only after the Civil War did today's prevailing view of immigration federalism—that federal immigration regulation displaces any state laws on the admission and expulsion of noncitizens—begin to emerge.").

366. The National Conference of State Legislatures compiles annual reports on state legislative activity regarding immigration as part of the Immigration Policy Project. *See generally State Laws Related to Immigration and Immigrants*, NAT'L CONF. ST. LEGISLATURES (Aug. 6, 2017), http://www.ncsl.org/research/immigration/state-laws-related-to-immigration-and-immigrants.aspx [https://perma.cc/TD2T-5R5F].

367. *See id.*

368. Memorandum from John Kelly, *supra* note 330, at 3.

369. Hillyard, *supra* note 357.

370. *See* EDWIN BLACK, IBM AND THE HOLOCAUST: THE STRATEGIC ALLIANCE BETWEEN NAZI GERMANY AND AMERICA'S MOST POWERFUL CORPORATION 21 (2001); Aebra Coe, *Ex-Ambassador Wants Ford, IBM Apartheid Liability Reviewed*, LAW360 (Mar. 21, 2016), https://www.law360.com/articles/773798 [https://perma.cc/G6MR-FL7Z]; Haya El Nasser,

discriminatory animus in the design of the vetting protocols and the database screening systems. That inquiry will likely start from an assessment of the disparate impact of identity-management technologies. Relatedly, challengers and the courts must contemplate the disparate impact of the algorithms themselves, the screening inputs that produce the results, and the discriminatory result of other data-driven decision-making tools, rather than in the personal animus of the screener. Judicial review should evolve to question analytical assumptions and to develop evaluative methods to interrogate the underlying algorithms informing the screening and vetting systems.

Challengers and federal courts must also become more aware of other types of discrimination that can be facilitated by digitalized vetting and screening protocols. Although "data driven discrimination" is not currently recognized, we can begin challenging the collection of data under privacy theories and attempt to limit the ways in which judgments can be made based on the analysis of such data. *Nelson*, for example, challenged data-driven decisions that imposed arbitrary definitions of suitability on moral proclivities rather than decision-making founded on a secure rational basis.[371]

Further, identity-management technologies and Algorithmic Jim Crow may force innovations in constitutional data-privacy theories. These may include, for example, asserting a reasonable expectation of privacy under the Fourth Amendment's prohibition of the search and seizure of data. The original complaints filed to enjoin LAWA's mandatory E-Verify database screening alleged a Fourth Amendment violation.[372] Among other challenges, the Chamber of Commerce argued that E-Verify required an unconstitutional search and seizure of an employee's personally identifiable information by Arizona employers.[373] The Fourth Amendment challenge, however, was not the driving force behind the litigation, was withdrawn by stipulation before the district court,[374] and was not before the Supreme Court in *Whiting*, which focused on the question of preemption.[375] Although the United States only challenged section 2(B) of Arizona's SB 1070 on preemption grounds, the American Civil Liberties Union (ACLU) had originally raised other constitutional claims, including a Fourth Amendment claim, to the implementation of section 2(B), which required mandatory biometric-database screening of those suspected of unlawful presence.[376]

---

*Papers Show Census Role in WWII Camps*, USA TODAY (Mar. 30, 2007), https://usatoday30.usatoday.com/news/nation/2007-03-30-census-role_n.htm [https://perma.cc/82GL-P5KR]; *see also supra* notes 132, 134 and accompanying text.

371. *See supra* notes 253–78 and accompanying text.

372. *See* Ariz. Contractors Ass'n v. Candelaria, 534 F. Supp. 2d 1036, 1061 (D. Ariz. 2008).

373. *Id.*

374. *Id.*

375. Chamber of Commerce v. Whiting, 563 U.S. 582, 594 (2011).

376. Valle del Sol v. Whiting, No. CV 10-1061-PHX-SRB, 2012 WL 8021265, at *2 (D. Ariz. Sept. 5, 2012).

Once again, the Fourth Amendment claim was not before the Supreme Court in *Arizona*, which also focused on preemption.[377]

It is important to note as well that, similar to *Korematsu*, the No Fly List challengers have relied on due process rather than equal protection. As in *Korematsu*, the government has defended the No Fly List as a national security program that does not target classifications of individuals, but, rather, targets risk. In his dissent in *Korematsu*, Justice Frank Murphy stated that "the order deprives all those within its scope of the equal protection of the laws as guaranteed by the Fifth Amendment."[378]

Of the relationship between due process and equal protection, William Eskridge has observed that "[t]he Due Process Clause announces a procedural norm."[379] To the extent that the Due Process Clause is recognized to carry a substantive element, Eskridge explains the courts demand "a fit between the reasonableness of the deprivation (whatever the process) and the 'law of the land.' The Equal Protection Clause requires the state to justify any difference in procedural or substantive treatment of one person vis-à-vis another."[380] Consequently, the Equal Protection Clause may be less useful than other constitutional options that can force political change, such as the Due Process Clause and the First Amendment.[381]

Eskridge suggests, however, that the Due Process Clause can secure important rights at the individual level.[382] He notes that our conception of due process is more elastic and can track changing standards of social progress.[383] Further,

> Perhaps the most fundamental value found in the Due Process Clause is the idea that the state is obligated to treat every person as a presumptively worthwhile human being who is entitled to respect and humane treatment. This principle is the key reason *Buck v. Bell* and [*Korematsu*] were wrongly decided."[384]

Eskridge signals that the time might be right to view equal protection and due process as "interchangeable and interdependent" in the vindication of individual rights.[385]

There are benefits to prevailing under an equal protection claim,[386] namely, "the Equal Protection Clause alone offers a minority group a

377. *See generally* Arizona v. United States, 567 U.S. 387 (2012).

378. Korematsu v. United States, 323 U.S. 214, 234–35 (1944) (Murphy, J., dissenting) ("In excommunicating them without benefit of hearings, this order also deprives them of all their constitutional rights to procedural due process. Yet no reasonable relation to an 'immediate, imminent, and impending' public danger is evident to support this racial restriction, which is one of the most sweeping and complete deprivations of constitutional rights in the history of this nation in the absence of martial law.").

379. William N. Eskridge, Jr., *Destabilizing Due Process and Evolutive Equal Protection*, 47 UCLA L. REV. 1183, 1187 (2000).

380. *Id.* at 1187–88.

381. *Id.* at 1214.

382. *Id.* at 1183.

383. *Id.* at 1210.

384. *Id.*

385. *Id.* at 1216.

386. *Id.*

potential constitutional jackpot at the *wholesale level*, that is, in challenges to an array of interconnected discriminations in state benefits as well as burdens."[387] Eskridge posits, however, that due process can yield similar wholesale benefits to protection as the Equal Protection Clause; under the Constitution, there is no theoretical or historical limit to extending wholesale rights to classes of individuals under a due process theory.[388] In fact, a "destabilizing due process" that offers multiple opportunities to challenge discrimination can result in an "evolutive equal protection."[389] Thus, the equal protection process may need to be pushed to evolve to realize new forms of discrimination once the Due Process Clause forces the federal courts to confront the unreasonableness of wholesale deprivations and the need to grant wholesale benefits to challengers alleging the infringement.

In the context of Algorithmic Jim Crow, however, the interrelationship between due process and equal protection is more pragmatic. Challenging algorithm-driven vetting and screening protocols under due process claims means demanding answers about the "black box" processes that may flag individuals as potential risks or threats.[390] As the algorithms and data-analytic processes become more transparent, equal protection violations can no longer be as easily disguised. This destabilization or disruption of government deprivations made possible by due process challenges can give new evaluative impetus to the evolution of the types of protections offered under the Equal Protection Clause.

Arguably, this process of destabilizing algorithmic due process is already occurring under due process and equal protection challenges, among others. The No Work List has been implicated in an equal protection challenge.[391] The No Vote List has been challenged[392] under section 2 of the Voting Rights

387. *Id.* ("[T]he Court's apparent classification-based approach offers a tremendous reward for groups that can persuade judges that the classification legally defining their group is suspect.").

388. *Id.* at 1216; *id.* at 1219 ("There may be no deep theoretical or even historical reason why the Due Process Clause's principles of fairness, antiarbitrariness, and dignity could not be applied on the wholesale level.").

389. *Id.* at 1186.

390. *See* PASQUALE, *supra* note 191, at 101–03; Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1260 (2008); Citron & Pasquale, *supra* note 196, at 3–4; 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); Hu, *supra* note 160, at 1759; Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 3 (2005).

391. *See* Puente Ariz. v. Arpaio, 76 F. Supp. 3d 833, 842 (D. Ariz. 2015), *rev'd in part, vacated in part*, 821 F.3d 1098 (9th Cir. 2016). In *Puente*, the plaintiffs challenged the constitutionality of state statutes "that criminalize the act of identity theft done with the intent to obtain or continue employment." *Id.* The state statutes in question required employers to use E-Verify and included provisions to ensure employers' participation in the E-Verify program: the "Legal Arizona Workers Act" and "Employment of Unauthorized Aliens." *Id.* at 844. The district court preliminarily enjoined the enforcement of the statutes, finding that the plaintiffs had demonstrated a likelihood of success on the merits of their equal protection claim. *Id.* at 854–56.

392. *See* Arcia v. Fla. Sec'y. of State, 772 F.3d 1335, 1348 (11th Cir. 2014) (reversing and remanding the district court's grant of judgment as a matter of law to the Secretary of State of

Act[393] and the "90 Day Provision" of the National Voter Registration Act.[394] The No Citizenship List has been challenged under both procedural due process and equal protection claims under the Fifth and Fourteenth Amendments,[395] as well as under the Fourth Amendment.[396] In addition, the subsequent litigation of the No Citizenship List was found to implicate the Tenth Amendment under the anticommandeering doctrine.[397] The No Fly List and Terrorist Watchlist have been challenged under multiple legal claims

---

Florida and declaring that the SAVE database screening program for voter purges were in violation of the 90-day provision of the National Voter Registration Act).

393. *Id.* The original complaint alleged that the SAVE database screening program aimed at removing noncitizens from voter registration rolls violated section 2 of the Voting Rights Act, asserting protection for "citizens . . . having 'less opportunity than other members of the electorate to participate in the political process and to elect the representatives of their choice.'" Complaint for Declaratory and Injunctive Relief at 18, Arcia v. Detzner, 908 F. Supp. 2d 1276 (S.D. Fla. 2012), *vacated*, 2015 WL 11198230 (S.D. Fla. Feb. 12, 2015) (No. 12-22282-CIV), 2012 WL 2308560 (quoting 42 U.S.C. § 1973 (2012)).

394. Complaint for Declaratory and Injunctive Relief, *supra* note 393, at 2. The original complaint also alleged that the SAVE database screening program aimed at removing noncitizens from voter registration rolls violated section 8(b)(1) of the National Voter Registration Act, also known as the "90 Day Provision," with plaintiffs asserting that the statute "prohibits the systematic purging of eligible voters from the official voter list for the State of Florida, within 90 days before the date of a primary or general election for Federal office." *Id.*

395. *See, e.g.*, Complaint at 1, Galarza v. Szalczyk, No. 10-cv-06815, 2012 WL 1080020 (E.D. Pa. Mar. 30, 2012), 2010 WL 4822758. In the original complaint, the plaintiff brought an "action under the Fourth, Fifth and Fourteenth Amendments to the United States Constitution, the Civil Rights Act of 1964 and the authority of *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971)." *Id.* Under the Fifth Amendment, the plaintiff alleged, "Issuance of an immigration detainer against Plaintiff based on his Hispanic ethnicity violated his right to be free from discrimination on the basis of ethnicity under the equal protection clause of the Fifth Amendment." *Id.* ¶ 94. Under the Fourteenth Amendment, the plaintiff alleged, "Treating Plaintiff as presumptively subject to detention and removal as an 'alien' on the basis of his Hispanic identity violated his rights under the equal protection clause of the Fourteenth Amendment." *Id.* ¶ 104. The plaintiff also alleged due process claims under the Fourteenth and Fifth Amendments. Under the Fourteenth Amendment, the complaint alleges that the defendants

> violated Plaintiffs right to due process of law guaranteed by the Fourteenth Amendment of the United States Constitution [by]: a) [i]mprisoning Plaintiff pursuant to a detainer issued on less than probable cause [and]; b) [f]ailing to give Plaintiff notice of and an opportunity to be heard regarding the grounds for the detainer before imprisoning Plaintiff pursuant to it.

*Id.* ¶ 114. Under the Fifth Amendment, the complaint alleged that the defendants "violated the Fifth Amendment by acting in the following ways: a) [v]iolating the terms of 8 U.S.C. § 1357, as interpreted by the courts, by issuing detainers on less than probable cause; b) [m]isrepresenting immigration detainers as orders for mandatory detention contrary to 8 C.F.R. § 287.7(a)." *Id.* ¶ 100.

396. *Id.* ¶ 90. In the original complaint, the plaintiff also brought an action under the Fourth Amendment, alleging that "[t]he issuance of the detainer against Plaintiff occurred without probable cause to believe that he was an 'alien' subject to detention and removal. That issuance constituted an unreasonable seizure in violation of Plaintiff's rights under the Fourth Amendment." *Id.*

397. *See* Galarza v. Szalczyk, 745 F.3d 634, 636 (3d Cir. 2014). In *Galarza*, the Third Circuit concluded that immigration holds are not mandatory commands, but rather—per the Tenth Amendment—discretionary for state agencies. *Id.* Therefore, the court reasoned, a previously dismissed § 1983 claim against the county that allegedly held the plaintiff was erroneously dismissed and remanded. *Id.* at 645.

and constitutional theories,[398] including procedural due process and substantive due process under the Fifth Amendment.[399]

Algorithmic Jim Crow may not be challenged successfully on equal protection grounds, but, rather, on other legal grounds, such as informational privacy grounds, the legal claim in *Nelson*. *Nelson* is especially useful to the analysis here as it involves a challenge to both a mandatory biometric ID program and the vetting protocols associated with the program.[400] Like the loyalty requirements imposed by the January 27, 2017, Order,[401] the vetting protocols challenged in Nelson also involved screening criteria to determine trustworthiness, morality, and suitability—criteria subsequently criticized by the Court as subjective and objectionable.[402]

Consequently, legal responses to Algorithmic Jim Crow may require preconceiving identity-management harms to encompass a broad range of legal theories. As in the No Fly List litigation, the government will likely defend disparate-impact consequences as justified based upon risk assessments, terroristic classifications, data-screening results deemed suspect, and characteristics establishing unsuitability.[403] These are classifications and characteristics not protected by equal protection jurisprudence. To acknowledge the harms emerging from Algorithmic Jim Crow, equality law should be broadened to recognize data-driven discrimination and recognition of algorithm- and big data-derived disparate impact, rather than limiting protection to only animus-based, classification-driven discrimination.

## CONCLUSION

Algorithmic Jim Crow regimes are distinguished from historic Jim Crow regimes in several significant respects. Algorithmic Jim Crow is cybersurveillance driven and dataveillance dependent, built around the transparency of biometric identity and other technologies of identity management, monitoring internet and social media activity and contact lists through telephony databases, database screening and digital watchlisting enforcement, and other emerging big data surveillance techniques. In contrast, traditional Jim Crow is law driven, built around the transparency of racial identity; monitoring economic, educational, political, and social

398. *See* Ibrahim v. Dep't of Homeland Sec., 62 F. Supp. 3d 909, 914 (N.D. Cal. 2014) (challenging Ibrahim's inclusion on the No Fly List under the First Amendment (freedom of association and freedom of religion), Fourth Amendment (freedom from unreasonable search and seizure), Fifth Amendment (procedural due process and substantive due process), and Fourteenth Amendment (equal protection)).

399. *See* First Amended Complaint paras. 52–72, *Ibrahim*, 62 F. Supp. 3d 909 (N.D. Cal. 2014) (No. C06-0545 WHA), 2006 WL 2330786; Complaint for Injunctive and Declaratory Relief paras. 216–255, Latif v. Holder, 28 F. Supp. 3d 1134 (D. Or. 2014) (No. 10-CV-750-BR).

400. NASA v. Nelson, 562 U.S. 134, 140–42 (2011).

401. *See supra* notes 298–99 and accompanying text.

402. *Nelson*, 562 U.S. at 143 n.5.

403. *See* Defendants' Cross-Motion for Summary Judgment, *Latif*, 28 F. Supp. 3d 1134 (D. Or. 2014) (No. 3:10-cv-00750-BR), 2015 WL 11347548.

activity; and utilizing traditional criminal enforcement and detention tools as well as small data surveillance techniques. Algorithmic Jim Crow describes an "equal but separate" system of de jure and de facto discrimination rather than the "separate but equal" discrimination of historic Jim Crow.

The goal of Algorithmic Jim Crow is not physical separation per se. Rather, all individuals subjected to an Algorithmic Jim Crow regime may be equally vetted through database screening and digital watchlisting systems. The separation, however, is achieved through data discrimination applied on the back end of screening and vetting protocols rather than overt social and economic discrimination and legal apartheid applied on the front end of segregationist regimes. The "equal but separate" impact of Algorithmic Jim Crow will likely manifest itself in the big data assessment of risk factors that purport to predict terroristic and criminal threat rather than segregation systems of racial or ethnic classification.

In other words, individuals will be at risk of disparate treatment on the basis of suspicious algorithmic results and anomalous data, or "foreignness" characteristics. Thus, disparate treatment stemming from cybersurveillance and dataveillance may not be characterized as traditional discrimination: discrimination on the basis of a historically protected class, for instance, race, color, ethnicity, national origin, and sex. This type of identity-management, technology-based discrimination may, therefore, fall outside current interpretations of the scope of the Fourteenth Amendment's Equal Protection Clause and outside the reach of the protection of civil rights statutes.

Algorithmic vetting and biometric identification, especially once deployed across an entire citizenry, will likely lead to discriminatory profiling and surveillance on the basis of suspicious digital data and internet and social media activity deemed "suspect," as well as classification-based discrimination, such as the isolation of those emigrating from Muslim-majority nations. These systems are likely to result in both direct and collateral discrimination on the basis of citizenship status, national origin, and religion, in particular. In addition, recent immigration-control policies and programs demonstrate the government's willingness to delegate screening and vetting duties to private actors, such as employers and local law enforcement, which can exacerbate issues of racial profiling and discrimination. This discrimination may face limited or lenient review by a federal judiciary that generally grants broad deference in matters of immigration and national security.

Because Algorithmic Jim Crow may appear to offer equality in theory, it may not be challenged successfully on equal protection grounds under the current equal protection framework. Thus, the jurisprudence must evolve to encompass new harms and recognize the disparate-impact harms of Algorithmic Jim Crow regimes. At the same time, Algorithmic Jim Crow must be challenged under other legal theories, including search and seizure of data under the Fourth Amendment, procedural due process and informational privacy rights under substantive due process guarantees of the Fifth and Fourteenth Amendments, First Amendment theories, and other statutory and constitutional theories. Wholesale disruptions to Algorithmic

Jim Crow under a wide range of legal theories will likely force an evolution of equal protection jurisprudence.