Washington University Law Review

Volume 96
Issue 6 *Trust and Privacy in the Digital Age*

2019

The Ironic Privacy Act

Margaret Hu
Kenan Institute for Ethics, Duke University; Washington and Lee University School of Law

THE IRONIC PRIVACY ACT

MARGARET HU*

ABSTRACT

This Article contends that the Privacy Act of 1974, a law intended to engender trust in government records, can be implemented in a way that inverts its intent. Specifically, pursuant to the Privacy Act's reporting requirements, in September 2017, the U.S. Department of Homeland Security (DHS) notified the public that record systems would be modified to encompass the collection of social media data. The notification justified the collection of social media data as a part of national security screening and immigration vetting procedures. However, the collection will encompass social media data on both citizens and noncitizens, and was not explicitly authorized by Congress. Social media surveillance programs by federal agencies are largely unregulated and the announcement of social media data collection pursuant to the reporting requirements of the Privacy Act deserves careful legal attention. Trust in the Privacy Act is at risk when the Act's notice requirements announce social media data collection and analysis systems under the guise of modifying record collection and retention protocols. This Article concludes that the social media data collection program proposed by DHS in September 2017 requires express legislative authorization.

* Margaret Hu, Kenan Visiting Professor, Kenan Institute for Ethics, Duke University (Fall 2019); Associate Professor of Law, Washington and Lee University School of Law. This work benefitted from the thoughtful feedback received from John Bagby, Danielle Citron, Deven Desai, Bob Gellman, Sue Glueck, Mark Graber, Janine Hiller, Rachel Levinson-Waldman, Ron Klain, Steve Miskinis, Angie Raymond, Neil Richards, Margaret Taylor, Ari Waldman, and Vanessa Zboreak. Many thanks to the participants of the *Washington University Law Review*'s Symposium: *Privacy and Trust in the Digital Age*; the Big Data Research Colloquium, "The Law & Ethics of Big Data"; and the Wake Forest Faculty Workshop. I am grateful for the editorial care shown by Nathan Finkelstein, Jenny Juehring, Kelly King, and the other dedicated members of the *Washington University Law Review*. My deepest gratitude to my excellent Research Assistants: Warren Buff, Mark Dewyea, Nick Martinez, Sean Moran, Chinny Sharma, and Matt Wyatt.

TABLE OF CONTENTS

INTRODUCTION

Social media surveillance[1] tools allow the government to collect, aggregate, and analyze billions of pieces of social media data points.[2] With approximately "2.3 billion active social media users[,]"[3] the ubiquity and public availability of social media[4] allows the government to monitor those

1. Multiple authors have helped to define and interrogate the impact of social media surveillance. *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019); SIVA VAIDHYANATHAN, ANTISOCIAL MEDIA: HOW FACEBOOK DISCONNECTS US AND UNDERMINES DEMOCRACY (2018); Rachel Levinson-Waldman, *Government Access to and Manipulation of Social Media: Legal and Policy Challenges*, 61 HOWARD L.J. 523 (2018); Danielle Keats Citron, *Fulfilling Government's 2.0's Promise with Robust Privacy* Protections, 78 GEO. WASH. L. REV. 822 (2010) [hereinafter Citron, *Government 2.0*]; Danah Boyd, *Social Network Sites as Networked Publics: Affordances, Dynamics and Implications, in* A NETWORKED SELF: IDENTITY, COMMUNITY AND CULTURE ON SOCIAL NETWORK SITES 39, 39–58 (Zizi Papacharissi ed., 2011); Christian Fuchs, *Social Media Surveillance, in* HANDBOOK OF DIGITAL POLITICS 395 (Stephen Coleman & Deen Freelon eds., 2016); CHRISTIAN FUCHS, SOCIAL NETWORKING SITES AND THE SURVEILLANCE SOCIETY (2009); Daniel Trottier & David Lyon, *Key Features of Social Media Surveillance, in* INTERNET AND SURVEILLANCE: THE CHALLENGES OF WEB 2.0 AND SOCIAL MEDIA 89, 89–105 (Christian Fuchs, Kees Boersma, Anders Albrechtslund & Marisol Sandoval eds., 2012); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1185 (2016); Jeramie D. Scott, *Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space*, 12 J. BUS. & TECH. L. 151 (2017); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 YALE L.J. 1180 (2017); Anupam Chander, *National Data Governance in a Global Economy*, U.C. DAVIS LEGAL STUDIES RESEARCH PAPER NO. 495 (2016); Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 UNIV. MIAMI L. REV. 559 (2015); FAIZA PATEL, RACHEL LEVINSON-WALDMAN, SOPHIA DENUYL, & RAYA KOREH, BRENNAN CTR. FOR JUSTICE, SOCIAL MEDIA MONITORING (2019) [hereinafter SOCIAL MEDIA MONITORING REPORT].

2. *See, e.g.*, Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat 'Score*,*'* WASH. POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html [https://perma.cc/5CRG-DSNP] (noting aggregation of data allows for analysis of "billions of data points, including arrest reports, property records, commercial databases, deep Web searches and [a] man's social-media postings"); *see also* RACHEL LEVINSON-WALDMAN, WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA (2013).

3. Hugh Handeyside, *To the Government, Your Latest Facebook Rant is Raw Intel*, ACLU BLOG (Sept. 26, 2016, 2:15 PM), https://www.aclu.org/blog/privacy-technology/internet-privacy/government-your-latest-facebook-rant-raw-intel [https://perma.cc/5SJ9-Z5YY].

4. Important research by privacy scholars has explored the challenges of protecting privacy rights in an Information Society. *See generally* JULIE COHEN, BETWEEN TRUTH AND POWER: LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019); WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018); DAVID GRAY, THE FOURTH AMENDMENT IN THE AGE OF SURVEILLANCE (2017); NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015); JULIE COHEN, CONFIGURING THE NETWORKED SELF (2012); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2008); MARK ANDREJEVIC, ISPY: SURVEILLANCE AND POWER IN THE INTERACTIVE ERA (2007); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE DIGITAL AGE (2006); Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441 (2010); Joshua A. T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981 (2014); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 35–40 (2013);

who "upload hundreds of millions of photos and send 500 million tweets each day, add 300 hours of video to YouTube each minute, and create six new Facebook profiles each second."[5] Nick Rasmussen, Director of the National Counterterrorism Center, explained: "[T]he work we're doing now with our partners in the intelligence community often doesn't involve really, really sensitive intelligence. It involves looking at Twitter and or looking at some other social media platform and trying to figure out who that individual behind that screen name, behind that handle might actually be and whether that person poses a threat . . . ."[6]

The advent of the digital age has brought the advent of Social Media Intelligence (SOCMINT) and Open-Source Intelligence (OSINT) to accompany other intelligence gathering tools, such as Human Intelligence (HUMINT) and Signals Intelligence (SIGINT).[7] The disclosures of former National Security Agency (NSA) contractor Edward Snowden in 2013 revealed the extent to which the intelligence community relies upon social media and internet surveillance,[8] and other data surveillance and cybersurveillance tools.[9] PRISM, for example, one of the first revelations, allowed the NSA and Federal Bureau of Investigation (FBI) to retrieve data from Microsoft, Yahoo, Google, Facebook, Skype, YouTube, Apple, and other companies.[10] Much research examining the legal consequences of the

Helen Nissenbaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7 ETHICS & BEHAV. 207 (1997); Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141, 142 (2014); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

5. Handeyside, *supra* note 3.

6. *Can the high-tech hunt for terrorists stop lone wolf attacks?*, PBS NEWSHOUR (Sept. 6, 2016, 8:15 PM), https://www.pbs.org/newshour/show/can-high-tech-hunt-terrorists-stop-lone-wolf-attacks [https://perma.cc/T7Z4-AGXV] (capturing PBS Correspondent Miles O'Brien's Interview with Nick Rasmussen, Director of the National Counterterrorism Center).

7. *Id.*

8. *See, e.g.*, JENNIFER GRANICK, AMERICAN SPIES: MODERN SURVEILLANCE, WHY YOU SHOULD CARE, AND WHAT TO DO ABOUT IT (2017); GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014); David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221 (2016); Jon L. Mills, *The Future of Privacy in the Surveillance Age*, *in* AFTER SNOWDEN: PRIVACY, SECRECY, AND SECURITY IN THE INFORMATION AGE 191 (Ronald Goldfarb ed., 2015); Margaret Hu, *Taxonomy of the Snowden Disclosures*, 72 WASH. & LEE L. REV. 1679 (2015) [hereinafter Hu, *Taxonomy*].

9. *See, e.g.*, Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498 (1988). Clarke describes dataveillance as the systematic monitoring or investigation of people's actions, activities, or communications through the application of information technology. *Id.* at 499.

10. *See, e.g.*, GREENWALD, *supra* note 8; Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program,* WASH. POST (June 7, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970cc b04497_story .html [https://perma.cc/Y2SF-3DKR] ("The National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets, according to a top-secret document obtained by The Washington Post."). *See generally* LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL

Snowden revelations has focused on activities that are explicitly recognized as foreign intelligence gathering and national security surveillance activities.[11] This Article, however, does not focus on foreign intelligence gathering or law enforcement data collection that is self-described by the federal government as surveillance. It also does not analyze the constitutional impact of social media data collection by the U.S. Department of Homeland Security (DHS) or other federal agencies.[12]

Instead, this Article focuses its attention on how social media intelligence-gathering programs conducted by the intelligence community may be replicated by DHS government record collection and retention protocols. Specifically, it aims to demonstrate how data surveillance, or dataveillance,[13] is increasingly bureaucratized in the digital age, often taking advantage of citizens' trust in day-to-day governance activities, such as the federal government's public announcement of its records collection and records maintenance protocols. To illustrate how social media intelligence objectives can be replicated under federal immigration law and policy, and

---

AGE (2016); GRANICK, *supra* note 8; Mills, *in* AFTER SNOWDEN, *supra* note 8; Hu, *Taxonomy*, *supra* note 8; Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SEC. J. 112 (2015); Stephen I. Vladeck, *Big Data Before and After Snowden*, 7 J. NAT'L SEC. L. & POL'Y 333 (2014).

11. Both preceding and following the revelations of Edward Snowden in June 2013, experts have offered a rich analysis of the legality of surveillance activities by the intelligence community. *See generally* DONOHUE, *supra* note 10; William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633 (2010); Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* 37 HARV. J.L. & PUB. POL'Y 757 (2014); Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014); Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465 (2015); Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 VA. L. REV. 1513 (2014); Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1 (2014); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269 (2012); Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951 (2006).

12. At the outset, it is critical to admit that a legal analysis of social media surveillance or open source intelligence gathering that relies on publicly available data is complicated significantly by the Fourth Amendment's current jurisprudence. Although a Fourth Amendment analysis goes beyond the scope of this Article, it is important to note that it could be argued that social media data collection by the government would not appear to fall within the protection of the Fourth Amendment's reasonable expectation of privacy test under Katz v. United States, 389 U.S. 347, 360 (1967), and the third-party doctrine. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979); *see also* United States v. Miller, 425 U.S. 435, 443 (1976). Under a straightforward reading of the third-party doctrine, it could be argued that information shared through a social media platform would not be considered private. Future scholarship will address how the recent Supreme Court decision in *Carpenter* forces a reexamination of the reach and scope of the Fourth Amendment in light of digital surveillance tools, including social media surveillance tools. Carpenter v. United States, 138 S. Ct. 2206 (2018).

13. *See, e.g.*, 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 . . . .").

through the record collection protocols of DHS, this Article focuses on a "Privacy Act of 1974; System of Records[:] Notice of Modified Privacy Act System of Records," published in the Federal Register by DHS on September 18, 2017 (September 2017 DHS Notice).[14] The Notice announced a modification of a specific system of records maintained by DHS: "DHS/USCIS [United States Citizenship and Immigration Services]-ICE [Immigration and Customs Enforcement]-CBP [Customs and Border Protection]-001 Alien File, Index, and National File Tracking System of Records."[15]

Under the public notice requirements of the Privacy Act of 1974,[16] in a Federal Register Notice published by DHS on September 18, 2017, DHS notified the public that this DHS record system would be modified to encompass social media data collection.[17] This social media data collection program should be understood as representing a bureaucratized evolution of digital surveillance or cybersurveillance.[18] Many new efforts to collect and analyze social media data are not labeled as surveillance or intelligence gathering programs. Rather, social media surveillance on citizens and noncitizens alike can occur administratively. As an outgrowth of the administrative state, they may at times fall outside of the legal restraints[19]

14. Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556 (Dep't of Homeland Sec. Sept. 18, 2017). The DHS Notice and other notices are interrelated, and expand social media data collection as part of immigration law and vetting procedures: (1) Privacy Act of 1974; DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 82 Fed. Reg. 44,198 (Sept. 21, 2017); (2) 60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration, 83 Fed. Reg. 13,806 (Dep't of State Mar. 30, 2018)); and (3) 60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa, 83 Fed. Reg. 13,807 (Dep't of State Mar. 30, 2018). *See also* SOCIAL MEDIA MONITORING REPORT, *supra* note 1.

15. Privacy Act of 1974, 82 Fed. Reg. at 43,556.

16. 5 U.S.C. § 552a (Supp. V 2017); *see also* Citron, *Government 2.0*, *supra* note 1; Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009); Kimberly A. Houser and Debra Sanders, *The Use of Big Data Analytics by the IRS: Efficient Solution or the End of Privacy as We Know It?*, 19 VAND. J. ENT. & TECH. L. 817 (2017).

17. *See supra* note 14, and *see infra* accompanying discussion in Parts II.B and III.A.

18. *See, e.g.*, LAWRENCE LESSIG, CODE VERSION 2.0 209 (2006) (describing cybersurveillance or "digital surveillance" as "the process by which some form of human activity is analyzed by a computer according to some specified rule . . . . [T]he critical feature in each [case of surveillance] is that a computer is sorting data for some follow-up review by some human."). An emerging evolution of U.S. cyber policy and the changing nature of cyber offensive or covert cyber activities may increasingly blend military cyber actions with other cybersurveillance programs. *See, e.g.*, Robert Chesney, *New Authorities for Military Cyber Operations and Surveillance, Including TMA [Traditional Military Activities]?*, LAWFARE (June 27, 2018, 2:46 PM), https://www.lawfareblog.com/new-authorities-military-cyber-operations-and-surveillance-including-tma [https://perma.cc/7MLF-XJ3U] (analyzing cyber provisions of the Senate version of the John McCain National Defense Authorization Act for Fiscal Year 2019 and noting provision that authorizes Cyber Command "to conduct surveillance targeting *private* Russian actors" in specific circumstance and questioning whether such activity should fall within NSA).

19. *See, e.g.*, Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435 (2008); Christopher Slobogin, *Government Data Mining and the Fourth*

imposed on the intelligence community by foreign intelligence surveillance law or the criminal procedure protections of the Fourth Amendment of the U.S. Constitution. Better understanding the routinized administration of social media surveillance as a screening and vetting procedure under immigration law, or as a homeland security or national security policy under DHS programs, can shed light on this emerging phenomenon.[20]

In the September 2017 DHS Notice, for instance, DHS explained that social media data now will be included in the Alien File (A-File).[21] The A-File is an official record of an immigrant applicant's visa and immigration history.[22] Alien registration numbers and related A-Files are created for

Amendment, 75 U. CHI. L. REV. 317 (2008); Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343 (2008).

20. Immigration scholars and other experts have increasingly focused their attention on immigration-related surveillance technologies that have been adopted by DHS. *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); Anil Kalhan, *Immigration Surveillance*, 74 MD. L. REV. 1 (2014); Fatma E. Marouf, *Alternatives to Immigration Detention*, 38 CARDOZO L. REV. 2141 (2017); Mark Noferi & Robert Khoulish, *The Immigration Detention Risk Assessment*, 29 GEO. IMMIGR. L.J. 45 (2014). After the terrorist attacks of September 11, 2001, scholars and experts called for greater scrutiny of immigration-related vetting procedures and registration systems. *See, e.g.*, Susan M. Akram & Kevin R. Johnson, *Race, Civil Rights, and Immigration Law After September 11, 2001: The Targeting of Arabs and Muslims*, 58 N.Y.Y. ANN. SURV. AM. L. 295 (2002); Victor C. Romero, *Decoupling Terrorist from Immigrant: An Enhanced Role for the Federal Courts Post 9/11*, 7 J. GENDER RACE & JUST. 201 (2003); Shoba Sivaprasad Wadhia, *Is Immigration Law National Security Law?*, 66 EMORY L.J. 669, 692 nn.142–43 (2017) (citing SHOBA SIVAPRASAD WADHIA & KAREEM SHORA, NSEERS: THE CONSEQUENCES OF AMERICA'S EFFORTS TO SECURE ITS BORDERS 9 (2009), https://www.adc.org/wp-content/uploads/2016/12/NSEERS-ADC-Report.pdf [https://perma.cc/GR8P-P8R4]; RIGHTS WORKING GRP. & CTR. FOR IMMIGRANTS' RIGHTS, PA. STATE UNIV.'S DICKINSON SCH. OF LAW, THE NSEERS EFFECT: A DECADE OF RACIAL PROFILING, FEAR, AND SECRECY (2012), https:// pennstatelaw.psu.edu/_file/clinics/NSEERS_report.pdf [https://perma.cc/BE4R-RSSP]). The National Security Entry-Exit Registration System (NSEERS) program was officially dismantled during the Obama Administration. *See, e.g.*, Shoba Sivaprasad Wadhia, *Shutting Down Special Registration*, MEDIUM (Dec. 11, 2016), https://link.medium.com/HJQnzkMr1Z [https://perma.cc/ZG5C-FWL5].

21. Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556 (Dep't of Homeland Sec. Sept. 18, 2017). Alien Files (A-File records) are defined as:

> [A] system of records contain[ing] information regarding transactions involving an individual as he or she passes through the U.S. immigration process, some of which may also be covered by separate Systems of Records Notices. DHS primarily maintains information relating to the adjudication of benefits, investigation of immigration violations, and enforcement actions in Alien Files (A-Files). Alien Files became the official file for all immigration records created or consolidated since April 1, 1944. Before A-Files, many individuals had more than one file with the agency. To streamline immigration recordkeeping, legacy Immigration and Naturalization Service issued each individual an Alien Number, allowing the agency to create a single file for each individual containing that individual's official immigration record. DHS also uses other immigration files to support administrative, fiscal, and legal needs.

Id.

22. Privacy Act; Alien File (A-File) and Central Index System (CIS) Systems of Records, 72 Fed. Reg. 1,755, 1,756 (Jan. 16, 2007) ("The A-File is the record that contains copies of information

immigrants and certain categories of non-immigrants who are granted employment authorization.[23] In addition to naturalized citizens and lawful permanent residents (green card holders), immigrant visa holders, asylees, and special immigrant juveniles, and student visa holders with optional practical training also possess A-File records by DHS.[24]

The September 2017 DHS Notice revealed that social media data can now be retained in the A-Files for both noncitizens and lawful permanent residents, as well as naturalized or foreign-born citizens of the United States. By some estimates, there are approximately forty-three million foreign-born individuals currently residing in the United States.[25] DHS retains A-File records after individuals gain naturalized U.S. citizenship.[26]

DHS claims that the September 2017 DHS Notice conforms to the existing protocol. In response to requests to clarify the Notice, DHS stated: "The notice did not announce a new policy. The notice simply reiterated existing DHS policy regarding the use of social media."[27] Yet, the Notice indicates that social media screening is emerging as a routinized aspect of DHS screening and vetting procedures. The Notice also signals how social media intelligence is increasingly becoming bureaucratized—treated not as a surveillance practice, but, rather, as a records collection practice.

This Article proceeds in four parts. Part I offers a brief overview of the Privacy Act and why experts have raised concerns that social media data collection promulgated by DHS is inconsistent with the law. Part II provides a summary of how DHS has engaged in social media monitoring since at least 2010. It also attempts to contextualize DHS social media surveillance practices within other algorithmic decisionmaking systems that are increasingly dependent upon mass data collection, including the gathering of social media data. Part III focuses on extreme vetting as a case study to

regarding all transactions involving an individual as he/she passes through the U.S. immigration and inspection process. Previously, legacy Immigration and Naturalization Services (INS) handled all of these transactions. Since the formation of DHS, however, these responsibilities have been divided among USCIS, ICE, and CBP. While USCIS is the custodian of the A-File, all three components create and use A-Files.").

23. *Id.*

24. *Id.*

25. *See* Riana Pfefferkorn, *On Social Media, How Can DHS Tell Who's An Immigrant?*, STAN. CTR. INTERNET & SOC'Y BLOG (Sept. 29, 2017, 11:40 PM), http://cyberlaw.stanford.edu/blog/2017/09/social-media-how-can-dhs-tell-who's-immigrant [https://perma.cc/RD24-GCM3] (citing Jie Zong, Jeanne Batalova & Jeffrey Hallock, *Frequently Requested Statistics on Immigrants and Immigration in the United States*, MIGRATION POLICY INSTITUTE (Feb. 8, 2018), https://www.migrationpolicy.org/article/frequently-requested-statistics-immigrants-and-immigration-united-states [https://perma.cc/R5VP-EEZW]).

26. *See supra* note 22.

27. Matt Novak, *US Homeland Security Says Tracking Social Media Is Nothing New*, GIZMODO (Sept. 28, 2017, 8:00 AM), https://gizmodo.com/us-homeland-security-says-tracking-social-media-of-immi-1818875395 [https://perma.cc/3GB8-X2SE].

better understand the data analytics-driven screening programs embraced by contemporary immigration and national security policies. Part IV explains why the reliance upon the Privacy Act's system of records notice (SORN) requirements to expand social media data collection undermines trust in federal administrative action and deserves careful legal attention.

Trust in the Privacy Act is at risk when the Act's required notice announces social media data collection and analysis systems under the guise of modifying record collection and retention protocols. This Article concludes that the social media data collection proposed by DHS requires express legislative authorization.[28] The Privacy Act does not authorize data collection. A Federal Register Notice announcing a system of records notice under the Privacy Act does not provide sufficient legal justification for mass social media data collection. Consequently, widespread and systematized social media data collection programs, such as the one proposed by DHS in the September 2017 DHS Notice, or proposed by any federal agency, require explicit congressional approval.

I. INTRODUCTION TO PRIVACY ACT AND SUMMARY OF CONCERNS RAISED BY THE DHS NOTICE: "PRIVACY ACT OF 1974; SYSTEM OF RECORDS" (SEPTEMBER 18, 2017)

Part I sets the factual and legal predicate for how one example of modern use of the Privacy Act of 1974 can be viewed as ironic. Part I.A provides an overview of the legislative background to the Privacy Act covering the (1) legislative history and (2) purpose and statutory requirements imposed on federal agencies. Part I.B summarizes the concerns of commenters—responding to modifications to the DHS/USCIS-ICE-CBP-001 Alien File, Index, and National File Tracking System of Records published by DHS in the Federal Register on September 18, 2017—involving the (1) constitutional impact, (2) Privacy Act and administrative law issues, and (3) apprehension regarding data collection, storage, and use stemming from the September 2017 DHS Notice.[29]

28. *See* SOCIAL MEDIA MONITORING REPORT, *supra* note 1, at 5.

29. Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556 (Dep't of Homeland Sec. Sept. 18, 2017).

A. Introduction to the Privacy Act of 1974

1. Legislative History and Amendment to the Privacy Act

Upon passage of the Privacy Act of 1974, the intention of the Act was made clear in a legislative statement entered by Congress: "Congress must act before sophisticated new systems of information gathering and retention are developed, and before they produce widespread abuses. The peculiarity of new complex technologies is that once they go into operation, it is too late to correct mistakes or supply our oversight."[30] Therefore, the Act aimed to "promote accountability, responsibility . . . [and prevent] illegal, unwise, overbroad, investigation and record surveillance of law-abiding citizens[.]"[31] To achieve this goal, Congress expressed its intent to "prevent the secret gathering of information on people or the creation of secret information systems or data banks on Americans by employees of the departments and agencies of the executive branch[,]" and to provide a method for publicly disclosing what confidential information was being stored on citizens and how that information would be used.[32]

The legislative history emphasizes the need to preserve citizens' privacy rights in light of digitized encroachments and includes this foresightful statement on the urgency for increased privacy protections under the law: "One of the most obvious threats the computer poses to privacy comes in its ability to collect, store, and disseminate information . . . Yet the increasing growth of information-gathering by Government and private organizations proceeds without any standards or procedures to regulate these organizations."[33] Senator Birch Bayh (D-Ind.) explained that the purpose of the Privacy Act was to help define the "basic right of every citizen to a sphere of privacy," to help the citizenry embrace the notion that a democratic society requires "freedom from unwarranted intrusion."[34] Congress stated the purpose of the Act was to "promote governmental respect for the privacy of citizens by requiring all departments and agencies of the executive branch and their employees to observe certain

30. 120 CONG. REC. 12,646 (May 1, 1974) (remarks of Sen. Ervin (D-N.C.) on S. 3418).

31. *Protecting Individual Privacy in Federal Gathering, Use and Disclosure of Information*, S. REP. NO. 93-1183, REPORT OF THE U.S. SENATE COMMITTEE ON GOVERNMENT RELATIONS TO ACCOMPANY S. 3418 TO ESTABLISH A PRIVACY PROTECTION COMMISSION, TO PROVIDE MANAGEMENT SYSTEMS IN FEDERAL AGENCIES AND CERTAIN OTHER ORGANIZATIONS WITH RESPECT TO THE GATHERING AND DISCLOSURE OF INFORMATION CONCERNING INDIVIDUALS, AND FOR OTHER PURPOSES 1 (1974) [hereinafter S. REP. NO. 93-1183].

32. *Id.* at 2–3.

33. 120 CONG. REC. 12,647 (May 1, 1974) (remarks of Sen. Ervin (D-N.C.) on S. 3418).

34. *Federal Data Banks, Computers, and the Bill of Rights: Hearing Before the Subcomm. on Constitutional Rights of the Comm. on the Judiciary, Part I*, 92nd Cong. 303 (1971) (statement by Sen. Bayh (D-Ind.), Member, S. Comm. on the Judiciary).

constitutional rules in the computerization, collection, management, use, and disclosure of personal information about individuals."[35] The Act, thus, recognized the need to "put specific limits on those who would gather and use this information."[36]

In 1988, the Privacy Act was amended to incorporate the Computer Matching and Privacy Protection Act (CMPPA).[37] The CMPPA prohibits computer matching of federally held data unless such matching is justified pursuant to statutory or executive directive authorities and is "relevant and necessary to accomplish" governmental objectives relating to the legal authority.[38] Specifically, the CMPPA applies to: federal engagement of computerized matching systems and electronic records comparisons, matching of categories of subjects and persons, the administration of a federal benefit program, and an intent to engage in a computerized matching activity.[39] The CMPPA is intended to complement the privacy goals of the Privacy Act, including the integrity of data use disclosure of data used by the federal government through computerized matching.[40]

2. Purpose of the Privacy Act and Statutory Requirements Imposed on Federal Agencies

The Privacy Act of 1974 was enacted to govern the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in "systems of records" by federal agencies.[41] A system of records is defined as "any records under the control of a federal agency from which information is retrieved by the name of the individual or by some . . . [identifier] . . . assigned to the individual."[42] The federal law prohibits the disclosure of information from a system of records absent the written consent of the subject individual, unless the disclosure is

35. S. REP. NO. 93-1183, *supra* note 31, at 1.

36. *Federal Data Banks, Computers, and the Bill of Rights: Hearing Before the Subcomm. on Constitutional Rights of the Comm. on the Judiciary, Part I*, 92nd Cong. 303, 304 (1971) (statement by Sen. Bayh (D-Ind.), Member, S. Comm. on the Judiciary).

37. 5 U.S.C. § 552a, Pub. L. No. 100-503 (1988).

38. § 552a(e)(1) (requiring that each federal agency must "maintain in its records only such information about an individual as relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.").

39. *Id.*

40. *See* Houser & Sanders, *supra* note 16, at 860–61 nn.316–20 (citing, *inter alia*, U.S. Dep't of Justice, *Overview of the Privacy Act of 1974*, *in* DEPARTMENT OF JUSTICE COMMENTARY § 3-17.000 3 (2015); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-44, COMPUTER MATCHING ACT: OMB AND SELECTED AGENCIES NEED TO ENSURE CONSISTENT IMPLEMENTATION 13 (2014); Privacy Act of 1974: Final Guidance Interpreting the Provisions of Public Law 100-503, The Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25,818 (Office of Mgmt. and Budget June 19, 1989)).

41. *See, e.g.*, § 552a(a)(5) (defining "system of records"); *see also supra* note 31.

42. § 552a(a)(5).

allowed under specified statutory exceptions.[43]

Passage of the Privacy Act was hastened by the Watergate investigation, and concerns by members of Congress that increasingly sophisticated methods of computerized database storage and querying could be abused. Specifically, "Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies that had been exposed during the Watergate scandal."[44] The Privacy Act was designed to "provide[] certain safeguards for an individual against an invasion of personal privacy" by the federal agencies.[45] In order to accomplish data privacy protections, especially in database management and the searching of databases by government officials, the Privacy Act enacted methods for handling an individual's confidential records and provided a civil remedies provision to authorize civil lawsuits against the federal government for Privacy Act violations.[46]

The Act generally provides the right of access to federal agency records where the person is a subject of those records.[47] That right to access one's records is judicially enforceable unless a federal agency is able to claim an exemption to the Privacy Act. The multiple exemptions available to federal agencies under the Privacy Act to prevent an individual's right of access to federal agency records will be discussed in more detail in Part IV.

Unlike exemptions, conditions of disclosure to third parties under the Privacy Act describe certain conditions that must be present for federal agencies to legally disclose information compiled on an individual to others[48]—including other federal agencies, contractors, and other private individuals.[49] To the extent that federal records are protected in part or in full from disclosure, a federal agency must claim that the records fall within one of the enumerated conditions of disclosure articulated by the Privacy Act. These conditions include, for example: statistical purposes by U.S.

43. § 552a(b)(1)–(12); *see also infra* note 255.

44. OFFICE OF PRIVACY AND CIVIL LIBERTIES, U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT 4 (2010), https://www.justice.gov/opcl/file/639731/download [https://perma.cc/BH4R-BW5J] (quoted in FAA v. Cooper, 132 S. Ct. 1441, 1462 (2012) (Sotomayor, J., dissenting)).

45. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a).

46. § 552a(g)(1)(D), (g)(4)(A).

47. *See* § 552a.

48. *See* § 552a(b)(1)–(12); *see also infra* note 255.

49. *See, e.g.*, Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556, 43,561 (Dep't of Homeland Sec. Sept. 18, 2017) (announcing "information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3)" to "F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records.").

Census Bureau and the Bureau of Labor Statistics;[50] routinized use within a U.S. government agency;[51] record archival purposes "as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government";[52] civil or criminal law enforcement purposes;[53] congressional investigations;[54] and to achieve other administrative objectives.[55]

Federal agencies must state "the authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary" when requesting information.[56] Importantly, the Privacy Act does not apply to all records of any given individual or citizen, but, rather, only applies to records held by a federal agency.[57]

Under the requirements of the Privacy Act, when a federal agency modifies its system of records, the agency must publish a notice in the Federal Register that describes the revision.[58] For instance, this Federal Register Notice must include: "each routine use of the records contained in the system, including the categories of users and the purpose of such use."[59] The Privacy Act provides that at least a thirty-day notice must be provided in the Federal Register of "any new use or intended use of the information in the system," along with an "opportunity for interested persons to submit written data, views, or arguments to the agency."[60] The September 2017 DHS Notice published in the Federal Register regarding the "Modified Privacy Act System of Records"[61] by DHS to include the collection of social media data, therefore, fell within these mandatory reporting requirements under the Privacy Act that dictated the publication of the change in collection and use of DHS's system of records.

50. § 552a(b)(4)–(5).
51. § 552a(b)(3).
52. § 552a(b)(6).
53. § 552a(b)(7).
54. § 552a(b)(9).
55. § 552a(b)(1).
56. § 552a(e)(3)(A).
57. § 552a(a)(4).
58. § 552a(e)(4).
59. § 552a(e)(4)(D).
60. § 552a(e)(11).
61. Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556 (Dep't of Homeland Sec. Sept. 18, 2017) ("ACTION: Notice of Modified Privacy Act System of Records.").

B. A Brief Overview of Selected Comments to DHS Notice "Privacy Act of 1974; System of Records" (September 18, 2017)

The September 2017 DHS Notice was highly controversial and resulted in over 2,900 comments submitted to DHS by the public.[62] Pursuant to the requirements of the Privacy Act that mandate disclosure of a federal agency's proposed revision to its system of records or establishment of a new system containing information on individuals,[63] DHS published the Notice to describe the collection and use of social media data.[64] DHS explained that the social media data would be used for the purposes of assessing and adjudicating immigration benefits, and for immigration investigations and enforcement.[65] DHS also indicated that other uses of the social media data would include investigatory purposes including criminal law enforcement and counterterrorism goals.[66]

1. Constitutional Law Concerns

The use of the Privacy Act's mandate to give public notice of a revision of DHS system records[67] to include social media data collection raises multiple legal concerns. These concerns include potential constitutional infringements, including the potential violation of First and Fourth Amendment rights. A close analysis of the constitutional impact of social media surveillance extends beyond the scope of this Article. It is important to note, however, that many commenters responding to the September 2017 DHS Notice raise concerns that are intersectional in nature. Several commenters note that social media surveillance combines constitutional concerns with technological capacity issues, such as whether the social

62. *See DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records, Docket ID: DHS-2017-0038*, REGULATIONS.GOV (Sept. 18, 2017), https://www.regulations.gov/docketBrowser?rpp=25&po=0&dct=PS&D=DHS-2017-0038&refD=DHS-2017-0038-0001 [https://perma.cc/V7LD-5VQR]; *see also* VICTORIA NEILSON, CHAIR, COMMITTEE ON IMMIGRATION & NATIONALITY LAW, NEW YORK CITY BAR, COMMENT ON NOTICE OF MODIFIED PRIVACY ACT SYSTEM OF RECORDS 3 (Oct. 20, 2017), https://s3.amazonaws.com/documents.nycbar.org/files/2017282Comments_on_System_of_Records_Notice_IMNAT_10.18.17.pdf [https://perma.cc/6TMP-RD8U] (noting over 2,400 comments were submitted by October 11, 2017).

63. § 552a(e)(4) ("subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records[.]").

64. Privacy Act of 1974, 82 Fed. Reg. at 43,556.

65. *Id.* at 43,556–57.

66. *Id.* at 43,557–63.

67. *See* § 552a(e)(4).

media data collected and analyzed can accurately serve the objectives articulated by DHS.[68]

Comments generated by the public and submitted to DHS in response to the Federal Register Notice include First Amendment concerns with chilling of speech and expressive freedoms, and infringing upon association rights.[69] Other First Amendment concerns include whether requests for social media handles and aliases could potentially jeopardize anonymous speech, and whether analysis of social media data may result in political and religious targeting.[70]

A coalition letter that included twenty-seven organizations—such as the ACLU, Brennan Center for Justice, Center for Democracy & Technology, the Electronic Frontier Foundation (EFF), and Human Rights Watch—and other expert responses, express concern regarding the warrantless seizure of data and mass cyber searches of social media information in violation of the Fourth Amendment.[71] A comment letter sent to DHS by the Electronic Privacy Information Center (EPIC) further shares the coalition's concern regarding the accuracy and integrity of the social media data collected.[72] Some commenters also note that the meaning of messages conveyed over social media might be difficult to interpret and discern.[73] Multiple comments express concern that naturalized U.S. citizens will be relegated to "second-class citizenship," as under the Notice the social media data may be retained on both immigrants and naturalized U.S. citizens.[74]

68. *See, e.g.*, *Coalition Letter Opposing DHS Social Media Retention*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Oct. 19, 2017), https://cdt.org/insight/coalition-lette r-opposing-dhs-social-media-retention/ [https://perma.cc/LK7C-22VJ] [hereinafter *Coalition Letter*]; Rotenberg & Scott, *infra* note 69, at 5.

69. *See* Comment submitted by Marc Rotenberg, Jeramie Scott, and the Electronic Privacy Information Center (EPIC) (Oct. 18, 2017), https://epic.org/apa/comments/EPIC-DHS-Social-Media-Info-Collection.pdf [https://perma.cc/P93D-FE3L] [hereinafter Rotenberg & Scott].

70. *See Coalition Letter*, *supra* note 68.

71. *See, e.g.*, Levinson-Waldman, *supra* note 1; Natasha Duarte, *Congress is Writing a Privacy Law. It Must Address Civil Rights*, CENTER FOR DEMOCRACY AND TECHNOLOGY (May 7, 2019) https://cdt.org/blog/congress-is-writing-a-privacy-law-it-must-address-civil-rights/ [https://perma.cc/2R5C-PT6U]; Cope & Schwartz, *infra* note 92; *Coalition Letter*, *supra* note 68; Rotenberg & Scott, *supra* note 69, at 8; Sellars, *infra* note 164; Patel & Panduranga, *infra* note 193.

72. Rotenberg & Scott, *supra* note 69, at 5–9; *see also* SOCIAL MEDIA MONITORING REPORT, *supra* note 1, at 5.

73. *See, e.g.*, *Coalition Letter*, *supra* note 68; Rotenberg & Scott, *supra* note 69; *see also* SOCIAL MEDIA MONITORING REPORT, *supra* note 1, at 4–5.

74. *See, e.g.*, *Coalition Letter*, *supra* note 68; NEILSON, *supra* note 62.

2. Privacy Act and Administrative Law Concerns

Multiple commenters note that the September 2017 DHS Notice appears to go beyond a simple modification of a "system of records." The Immigration and Nationality Law Committee of the New York City Bar, for instance, observes in its comment that the DHS Notice issued sweeping changes to the categories of persons covered by the system to include, for example, "associates" who may include immigration attorneys and other counsel.[75] The New York City Bar further notes that the modification of records did not appear to be a modification at all, but, rather, appeared to be a new form of system information that may require congressional authorization.[76] The New York City Bar voices administrative procedure concerns with the Notice, and whether the Privacy Act has been honored in spirit, even though it may have been honored under the letter of the law.[77]

3. Data Collection, Storage, and Use Concerns

Civil rights organizations and others raise a particular concern about the vagueness of the September 2017 DHS Notice. The Notice, for instance, failed to define "social media" or "search results."[78] The Notice also failed to limit retention of the social media data, thus allowing for the default: 100 years for the storage of the social media data held within the DHS A-Files.[79] The coalition notes that the failure to explain with any specificity how exactly the social media data would be used, currently and into the future, raises a concern regarding how such data might invite discrimination and data abuse, negative inferences, and may chill expressive and associational freedoms.[80]

Multiple comments reflect deep reservations about the new social media

75. NEILSON, *supra* note 62, at 4.
76. *Id.* at 2–5.
77. *See id.* at 3.
78. *Coalition Letter*, *supra* note 68.
79. *Id.*
80. *Id.* Important research has been published on the potential harms of predictive analytics, and the inferential harms that may flow from big data scoring/risk assessment systems and algorithmic decisionmaking. *See, e.g.*, PASQUALE, *supra* note 4; Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV 671 (2016); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 3–4 (2014); 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); Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579 (2014); Jennifer C. Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327, 328–30 (2014); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1260 (2007). Other scholars have focused critical research on the relationship between data production and social media data, and protection of expressive freedoms. *See, e.g.*, Jack M. Balkin, *Free Speech is a Triangle*, 118 COLUM. L. REV. 2011 (2018); Jane Bambauer, *Is Data Speech*, 66 STAN. L. REV. 56 (2014).

data collection activities by the federal government in light of unanswered questions. These questions include: whether or not the social media collection was indeed a storage of records or whether the social media information would be collected for the purposes of new intelligence products;[81] how the storage of the data in the A-Files for up to one-hundred years could impact future use in automated decision making and algorithmic risk assessment;[82] and whether such social media surveillance might increase the risk of data misuse and abuse without evidence of the benefits to national security.[83] Some commenters suggest adding the ability to correct, access, and even destroy data collected in order to prevent power imbalances, and to better ensure fairness and accuracy for important data-driven decisions.[84] Finally, several commenters express a concern that the new social media collection protocols may effectively relegate naturalized U.S. citizens to second-class citizenship status,[85] not only as a matter that may implicate constitutional law, as mentioned above, but also as a matter of data retention and use. These commenters point out that questions remain regarding whether social media surveillance would continue and for how long after an individual might become a naturalized U.S. citizen.[86]

II. BRIEF HISTORY OF SOCIAL MEDIA INTELLIGENCE GATHERING BY DHS

To better understand how DHS uses social media data to serve broader intelligence objectives beyond immigration screening and vetting, Part II provides the following historical background: (A) the initial attempts by DHS to utilize social media data; (B) history of how DHS integrated social media data collection into an official federal agency policy; and (C) context for why social media intelligence by the intelligence community is considered legally and programmatically distinct from social media data collection by DHS for its records system. Yet, as will be explored in more detail in Parts III and IV, this Article invites further discussion on how this distinction may be obscuring the true privacy law impact of social media data collection.

A. DHS Social Media Monitoring Pilot Programs

The federal government publicly declared that it would capture social media technologies not for express surveillance purposes, but, rather, in the

81. *See Coalition Letter*, *supra* note 68, at 5.
82. *See id.* at 6.
83. *See id.*
84. *See* Duarte, *supra* note 71.
85. *See* NEILSON, *supra* note 62, at 4; *Coalition Letter*, *supra* note 68.
86. *See Coalition Letter*, *supra* note 68.

service of executive branch engagement with the public shortly after the election of President Barack Obama. In January 2009, Obama initiated a "Transparency and Open Government" initiative.[87] Also referred to as "Government 2.0," the initiative mandated the adoption of social media technology by federal agencies, in part, in order to "put information about [governmental] operations and decisions online . . . ."[88] Privacy scholars such as Danielle Keats Citron observed that an increased use of social media by the executive branch ushered in the promise of many potential beneficial uses, including: "to broadcast updates on pressing matters[,] to post research data . . . [and] to facilitate discussions between agencies and citizen-experts on policy matters and will surely entice people who might otherwise not engage with government to join those discussions."[89] At the same, Citron predicted that the federal government's use of social media would introduce a host of unprecedented privacy concerns.[90] With a broader engagement of social media data, the federal government would likely use social media surveillance. Citron observed that "[n]othing prevents agencies from collecting, analyzing, and distributing individuals' *social-media data* for law enforcement, immigration, benefits determinations, and other [national security and non-national security] purposes."[91]

Citron's warning proved prescient. On a pilot program basis, DHS officially commenced its experimentation with social media surveillance as early as 2010.[92] In 2010, through social media monitoring, DHS "targeted public reactions to the earthquake in Haiti, the Winter Olympics in Vancouver and the Deepwater Horizon oil spill."[93] DHS was particularly interested in harnessing social media monitoring to enhance its "situational

87. Transparency and Open Government: Memorandum for the Heads of Executive Departments and Agencies, 74 Fed. Reg. 4,685 (Jan. 21, 2009).

88. *Id.*

89. *See* Citron, *Government 2.0*, *supra* note 1, at 825 (internal citations omitted).

90. *Id.* at 826.

91. *Id.*

92. *See, e.g.*, Sophia Cope & Adam Schwartz, *DHS Should Stop the Social Media Surveillance of Immigrants*, EFF: DEEPLINKS BLOG (Oct. 3, 2017), https://www.eff.org/deeplinks/2017/10/dhs-should-stop-social-media-surveillance-immigrants [https://perma.cc/V6WQ-3K3U]. The Brennan Center for Justice's timeline of social media screening activities related to DHS vetting also provides an excellent resource to better understand the historical development of social media surveillance by DHS. *ICE Extreme Vetting Initiative: A Resource Page, Chronology of Social Media Monitoring: Timeline of Social Media Monitoring for Vetting by DHS and the State Department*, BRENNAN CTR. FOR JUST. (Sept. 9, 2019), https://www.brennancenter.org/analysis/timeline-social-media-monitoring-vetting-department-homeland-security-and-state-department [https://perma.cc/AP27-GD83].

93. G.W. Schulz, *Homeland Security Office OKs Efforts to Monitor Threats Via Social Media*, REVEALNEWS (Nov. 15, 2012), https://www.revealnews.org/article/homeland-security-office-oks-efforts-to-monitor-threats-via-social-media/ [https://perma.cc/8LPV-VNMT].

awareness capacities."[94] Situational awareness[95] is defined by the Homeland Security Act of 2002 as: "[I]nformation gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management decisionmaking."[96]

Also, in 2010, the EFF obtained documents through the Freedom of Information Act that revealed DHS officials in the Office of U.S. Citizenship and Immigration Services were instructed on how to "friend" immigrants on Facebook in order to monitor social media details on their background.[97] Other DHS social media monitoring programs appeared to focus on forecasting homeland security threats. As a result of a Freedom of Information Act request for information by EPIC in 2012, it was revealed that DHS monitored the use of "keywords and phrases" on various social media sites in order to detect "signs of terrorist or other threats against the U.S."[98] As part of its social media monitoring initiative, DHS's National Operations Center signed up for a Twitter profile (twitter.com/DHSNOCMMC1) with the handle @DHSNOCMMC1.

Other agencies also announced initiatives designed to monitor or analyze social media in order to forecast national security risks. In 2012, for example, the U.S. Department of Defense, Defense Advanced Research Projects Agency (DARPA), announced an initiative titled: "Forecasting Dynamic Group Behavior in Social Media."[99] DARPA solicited an automated tool that analyzed social media data to predict terrorism. It explained that: "Many online communities enable the creation of virtual teams, which evolve over time. Among these communities and teams are terrorist and other criminal organizations."[100] In order to "forecast[] dynamic group behavior in social media[,]" DARPA explained that it

94. *Id.*; *see also* OFFICE OF SCIENCE AND TECHNOLOGY, DEP'T OF HOMELAND SEC., USING SOCIAL MEDIA FOR ENHANCED SITUATIONAL AWARENESS AND DECISION SUPPORT (2014), https://www.dhs.gov/sites/default/files/publications/Using%20Social%20Media%20for%20Enhanced%20Situational%20Awareness%20and%20Decision%20Support.pdf [https://perma.cc/ET3T-ZGLU] [hereinafter USING SOCIAL MEDIA].

95. *See* USING SOCIAL MEDIA, *supra* note 94.

96. Homeland Security Act of 2002, 6 U.S.C. § 321d(a) (2006).

97. Jennifer Lynch, *Applying for Citizenship? U.S. Citizenship and Immigration Wants to Be Your 'Friend*,' EFF (Oct. 12, 2010), https://www.eff.org/deeplinks/2010/10/applying-citizenship-u-s-citizenship-and [https://perma.cc/2648-FR6Y].

98. DEP'T OF HOMELAND SEC., NATIONAL OPERATIONS CENTER MEDIA MONITORING CAPABILITY DESKTOP REFERENCE BINDER (2011), https://epic.org/foia/epic-v-dhs-media-monitoring/Analyst-Desktop-Binder-REDACTED.pdf [https://perma.cc/WSA2-SSRK].

99. DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, 12.B SMALL BUSINESS TECHNOLOGY TRANSFER PROGRAM (STTR) PROPOSAL SUBMISSION INSTRUCTIONS, https://www.acq.osd.mil/osbp/sbir/solicitations/sttr2012b/darpa12B.htm [https://perma.cc/C37L-SB62].

100. *Id.*

envisioned tools that had the capacity to scan over one million people, over 1,000 groups, and over 100,000 postings per day.[101]

In 2012, the FBI released a Request for Information, soliciting information on the development of a tool that would assist the agency in using social media and internet surveillance through web scraping and analysis of other open-source data. The FBI explained: "The application must have the ability to rapidly assemble critical open source information and intelligence that will allow [the FBI's Strategic Information and Operations Center] to quickly vet, identify and geo-locate" potential threats.[102] The FBI further requested the ability to automatically search and scrape data off social media and news sites based on agent's queries, and the ability to display alerts on geo-spatial maps in order to isolate threats.[103] Media reports indicate that the FBI has continued to acquire and pursue the acquisition of large-scale social media monitoring tools.[104]

B. DHS Social Media Monitoring as Official Policy: DHS Directive 110-01

DHS officially launched its social media monitoring policy on June 8, 2012, through the publication of DHS Directive 110-01: "Privacy Policy for Operational Use of Social Media" (Directive).[105] DHS provided the following legal authorities for the Directive:

> A. Public Law 107-347, "E-Government Act of 2002," as amended, Section 208 [44 U.S.C. § 3501 note][;]
>
> B. Title 5, United States Code (U.S.C.), Section 552a, "Records Maintained on Individuals" [The Privacy Act of

101. *Id.*

102. STRATEGIC INFO. & OPERATIONS CTR., FED. BUREAU OF INVESTIGATION, REQUEST FOR INFORMATION (RFI) (Jan. 19, 2012), https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=c65777356334dab8685984fa74bfd636&_cview=1 [https://perma.cc/4JTD-JCEE] (follow "RFI" hyperlink).

103. *Id.*

104. *See, e.g.*, Jeff Horwitz & Dustin Volz, *FBI Surveillance Proposal Sets Up Clash with Facebook: Agency Solicits Vendor Proposals to Collect Data from Facebook, Other Social Media to Head Off Safety Threats*, WALL ST. J. (Aug. 8, 2019, 8:15 PM), https://www.wsj.com/articles/fbi-and-facebook-potentially-at-odds-over-social-media-monitoring-11565277021 [https://perma.cc/XEW4-6XU3]; Joseph Cox, *SocioSpyder: The Tool Bought by the FBI to Monitor Social Media*, VICE (Feb. 23, 2016, 9:55 AM), https://www.vice.com/en_us/article/8q8g73/sociospyder-the-tool-bought-by-the-fbi-to-monitor-social-media [https://perma.cc/7YU4-EPQG] (citing FEDERAL PROCUREMENT DATA SYSTEM, https://www.fpds.gov/ezsearch/fpdsportal?q=allied+associates+CONTRACTING_AGENCY_NAME:%22FEDERAL+BUREAU+OF+INVESTIGATION%22&s=FPDS&templateName=1.4&indexName=awardfull&x=0&y=0).

105. DEP'T OF HOMELAND SEC., DHS DIRECTIVE 110-01, PRIVACY POLICY FOR OPERATIONAL USE OF SOCIAL MEDIA (June 8, 2012), https://www.dhs.gov/xlibrary/assets/foia/110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf [https://perma.cc/G5GV-UZBQ].

> 1974, as amended][;]
>
> C. Title 6 U.S.C. Section 142, "Privacy officer"[;]
>
> D. Title 44, U.S.C., Chapter 35, Subchapter III, "Information Security" [The Federal Information Security Management Act of 2002, as amended (FISMA)][;]
>
> E. Delegation 13001, "Delegation to the Chief Privacy Officer[.]"[106]

The Directive explains that each DHS component head has the discretion to determine how to deploy social media monitoring tools and that "[c]omponent heads work with the [DHS] Chief Privacy Officer to ensure that Department operational activities using social media follow DHS privacy policy and procedures, thereby enhancing the overall consistency of privacy protections across DHS."[107] In a six-month period in 2012, over 9,300 "item-of-interest" reports were generated by the DHS social media monitoring program.[108]

From the adoption of the Directive under the Obama Administration in June 2012 until the commencement of the Trump Administration in January 2017, DHS engaged in the adoption of multiple social media screening tools. In February 2017, the DHS Office of Inspector General issued a report titled, *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success*.[109] The report revealed that in December 2015, for instance, DHS adopted a social media screening tool that facilitated both manual and automatic screening of unspecified individuals submitting applications to DHS in order to "examine the feasibility" of the tool.[110] The report explained that DHS utilized a "social media analytics tool" that "covers a large number of social media platforms, has access to third-party information providers, and can access web-based information."[111] By April 2016, DHS began testing an additional social

106. *Id.* at 1–2.

107. *Id.* at 2.

108. Emily Stanton, *Department of Homeland Security Uses Twitter for Monitoring Citizens*, US NEWS BLOG (July 18, 2013, 12:43 PM), https://www.usnews.com/news/blogs/washington-whispers/2013/07/18/department-of-homeland-security-uses-twitter-for-monitoring-citizens [https://perma.cc/T379-SQMT].

109. DEP'T OF HOMELAND SEC., OFFICE OF INSPECTOR GENERAL, OIG-17-40, DHS' PILOTS FOR SOCIAL MEDIA SCREENING NEED INCREASED RIGOR TO ENSURE SCALABILITY AND LONG-TERM SUCCESS (Feb. 27, 2018), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf [https://perma.cc/QTA8-H5AF] [hereinafter DHS' PILOTS FOR SOCIAL MEDIA SCREENING].

110. *Id.* at 2.

111. *Id.* at 2, n.6.

media screening tool that was developed by DARPA in order to screen nonimmigrant visa holders.[112]

On June 23, 2016, Customs and Border Protection (CBP) within DHS issued a Federal Register notice titled, "Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization."[113] Under the Federal Register notice, issued under the Paperwork Reduction Act, CBP proposed the collection of social media data of travelers arriving through the Visa Waiver Program as part of the Arrival and Departure Record, Nonimmigrant Visa Waiver Arrival/Departure, and Electronic System for Travel Authorization (ESTA), including adding optional data fields on the DHS Form I-94 and DHS Form I-94W.[114] Independently, in August 2016, Immigration and Customs Enforcement (ICE) within DHS began the pilot testing of a social media screening tool to screen nonimmigrant visa holders that was intended to complement background "checks conducted in conjunction with the Department of State and help identify potential derogatory information not found in Government databases."[115]

The report noted that pilot tests of social media screenings by DHS up until that point had "lack[ed] criteria for measuring performance to ensure they meet their objectives."[116] Without further evidence and testing information, the report concluded that the tests "provide limited information for planning and implementing an effective, department-wide future social media screening program."[117]

C. SOCMINT: Social Media Intelligence and Algorithmic Decision-making

The intelligence community (IC) is comprised of sixteen IC components that are coordinated under the umbrella of the White House Office of the Director of National Intelligence (ODNI).[118] The IC includes the National Security Agency (NSA), Central Intelligence Agency (CIA), and FBI.[119] DHS includes one office, the Office of Intelligence and Analysis, that provides DHS with intelligence information and coordinates intelligence activities with the other IC components, as well as "fusion centers" that are

112. *Id.* at 2–3.

113 Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W) and Electronic System for Travel Authorization, 81 Fed. Reg. 40,892 (Customs and Border Prot. June 23, 2016).

114. *Id.*

115. DHS' PILOTS FOR SOCIAL MEDIA SCREENING, *supra* note 109, at 3–4.

116. *Id.* at 1.

117. *Id.*

118. *Collaboration*, OFF. OF DIRECTOR OF NAT'L INTELLIGENCE, https://www.dni.gov/index.php/how-we-work/collaboration [https://perma.cc/C8GH-Y8YJ].

119. *Id.*

tasked with the collection and analysis of "threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners."[120] Because other non-IC components of DHS have been tasked with the collection of social media data, the collection of social media data by non-IC components may not be formally identified as "Social Intelligence" or SOCINT *per se*. Consequently, some refer to the collection as social media tracking or social media monitoring, as the collection and use of DHS social media data is not fully known or understood. Further, some experts would contend that the social media data collection is not appropriately characterized as "intelligence."[121]

As DHS Directive 110-01 allows each component to establish its own policies and programs regarding the operational use of social media,[122] it is instructive to examine how one component, CBP, appears to be utilizing social media data in its intelligence gathering operations. On September 21, 2017, CBP announced a modification of the "System of Records" under the Privacy Act of 1974. The newly created CBP Intelligence Records System (CIRS) is intended to aggregate immigration, law enforcement, national security, and publicly available data, such as social media data, to generate CBP intelligence reports by the CBP Office of Intelligence (OI).[123] The CIRS will deploy algorithmic decision-making and predictive tools, including the "Analytical Framework for Intelligence (AFI)" and "Intelligence Reporting System (IRS)."[124] The systems apparently will rely upon complex algorithms to assess identity, social and organizational relationships, and automated threat-risk assessments.

The CIRS will focus on identifying "commonalities" that allow the CBP Intelligence Office to develop "a DHS-generated intelligence product that may lead to further investigation or other appropriate follow-up action by CBP, DHS, or other federal, state, or local agencies."[125] The report will also heavily focus on analysis of associational data.[126] The Notice explains that the analysis will rely upon biographic, biometric, criminal and investigatory records, and other government documents.[127] By specifying that the data

120. *Fusion Centers*, DHS, https://www.dhs.gov/fusion-centers [https://perma.cc/8QPE-C85R]; *see also, e.g.*, Citron and Pasquale, *supra* note 4.

121. *See, e.g.*, *Coalition Letter*, *supra* note 68; Rotenberg & Scott, *supra* note 69 (experts submitting comments in response to the DHS's Notice of Modification of System of Records, Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556 (Sept. 18, 2017), use the terms "social media screening" and "social media collection" and do not use the term "social media intelligence").

122. *See Coalition Letter*, *supra* note 68; Rotenberg & Scott, *supra* note 69.

123. Privacy Act of 1974; DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 82 Fed. Reg. 44,198 (Sept. 21, 2017).

124. *Id.* at 44,199.

125. *Id.*

126. *Id.* at 44,198.

127. *Id.* at 44,200.

analyzed will also include publicly available information, the CIRS will allow for the inclusion of social media analysis.

The Notice explains that the scope of those who can be targeted for an investigation includes those who may be "associated" with border security or CBP law enforcement goals.[128] Targets for investigation can also include individuals who possess "a potential nexus to national security, CBP's law enforcement responsibilities, or homeland security in general[.]"[129] This suggests the system can collect data from citizens and noncitizens. The underlying data and intelligence reports generated by the system can be shared with other law enforcement and intelligence agencies.[130] Finally, it appears that the system can inform A-File records and, therefore, can be used to guide analytics for algorithmic decision-making systems developed by other DHS components. In response to the CIRS proposal, EPIC submitted a comment to the DHS criticizing the system for the security threat created by compiling the data into a centralized database, the broad scope of data to be stored, and the impact the system would have on citizens not under investigation.[131]

III. EXTREME VETTING

The algorithmic decisionmaking tools acquired by DHS externally through private contractors and internally through DHS integrated database systems are dependent upon massive volumes of data. Social media data is seen as a critical component of the success of these tools. One way to better understand this is to look carefully at the extreme vetting proposal that stemmed from what was referred to as the "Muslim ban" or the "travel ban." In Part III, the discussion will (A) provide a brief history of how social media data collection is considered one of the data backbones of what has been referred to as the "extreme vetting" of immigrants; (B) describe the predecessor tools that "extreme vetting" is built upon; and (C) explain how social media monitoring is reflected in the Visa Lifecycle Vetting Initiative, an incarnation of "extreme vetting" that appears to combine manual vetting with automated vetting systems.

128. *Id.*

129. *Id.*

130. "Consistent with DHS's information sharing mission, information stored in the DHS/CBP-024 CIRS System of Records may be shared with other DHS Components . . . [and] DHS/CBP may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses[.]" *Id.* at 44,199.

131. Comment Submitted to DHS by Electronic Privacy Information Center responding to 82 Fed. Reg. 44,198, "Privacy Act of 1974; DHS/CBP-024 Intelligence Records System (CIRS) System of Records," (Oct. 23, 2017), https://www.epic.org/apa/comments/EPIC-CBP-Intelligence-Records-System-Comments.pdf [https://perma.cc/8DCL-4LB4].

A. Muslim Ban and Social Media Screening of Immigrants

On December 7, 2015, then-presidential candidate Donald J. Trump published a "Statement on Preventing Muslim Immigration" on his campaign website.[132] Trump explained that he was "calling for a total and complete shutdown of Muslims entering the United States until our country's representatives can figure out what . . . is going on."[133] The campaign later explained that the temporary ban on entry would permit the government to execute an assessment of immigration procedures, and "suspend immigration from regions linked with terrorism . . . ."[134] Shortly before his election, Trump also announced a proposal for the "extreme vetting" of immigrants and refugees.[135] 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."[136]

One week after his inauguration, President Trump signed Executive Order 13,769, on January 27, 2017, titled "Protecting the Nation from Foreign Terrorist Entry into the United States,"[137] the first of several documents referred to as the "travel ban" or the "Muslim ban." The first travel ban incorporated multiple screening requirements that mandated the

132. *See* Megan Trimble, *Trump 'Muslim Ban' Post Now Missing From Campaign Website*, US NEWS (May 9, 2017, 11:29 AM), https://www.usnews.com/news/national-news/articles/2017-05-09/trump-muslim-ban-post-missing-from-campaign-website-after-reporter-question [https://perma.cc/E24G-U8XG]; 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* Shoba Sivaprasad Wadhia, *National Security, Immigration and the Muslim Bans*, 75 WASH. & LEE L. REV. 1475, 1478–80 (2018) (contending that "backdoor bans" that restrict immigration on the basis of nationality can be constructed through "administrative processing"); Peter Margulies, *Bans, Borders, and Justice: Judicial Review of Immigration Law in the Trump Administration*, 2018 MICH. ST. L. REV. 1, 35–48 (2018) (arguing for a more searching judicial review of "extreme vetting" and the need to recognize the significant long-term impact of "extreme vetting").

133. Peters & Wooley, *supra* note 132.

134. Donald J. Trump (@realDonaldTrump), TWITTER (June 25, 2016, 7:37 PM), https://twitter.com/realdonaldtrump/status/746895065591783424?lang=en [https://perma.cc/H3AL-F4HX].

135. *See* Margaret Hu, *Algorithmic Jim Crow,* 86 FORD. L. REV 633, 635 (2017) [hereinafter Hu, *Algorithmic Jim Crow*]; Margaret Hu, *Crimmigration-Counterterrorism*, 2017 WISC. L. REV 955, 962 (2017) [hereinafter Hu, *Crimmigration-Counterterrorism*]. On August 15, 2016, then candidate Trump announced at a campaign rally that if elected President he would implement what he referred to as "extreme vetting" of refugees and immigrants for national security purposes. *See* Jeremy Diamond, *Trump Proposes Values Test for Would-Be Immigrants in Fiery ISIS Speech*, CNN POLITICS (Aug. 15, 2016, 9:39 PM), https://www.cnn.com/2016/08/14/politics/donald-trump-isis-fight/index.html [https://perma.cc/ZD4K-HLZV]. Then-candidate Trump explained: "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." *Id.*

136. Peters & Wooley, *supra* note 132.

137. Exec. Order No. 13,769, 82 Fed. Reg. 8,977 (Feb. 1, 2017).

implementation of extreme vetting.[138] Then-Secretary of DHS John Kelly testified at a hearing before the U.S. House Homeland Security Committee on February 7, 2017, that extreme vetting would include seeking the social media passwords in order to screen social media activity and other types of screening, such as web browsing history.[139] On March 6, 2017, in response to litigation surrounding the first travel ban, President Trump issued a revised Executive Order under the same title as the first travel ban, Executive Order 13,780, which left the extreme vetting provisions of the first travel ban in place and appeared to expand several vetting protocols.[140]

As a method of implementing extreme vetting, the U.S. Department of State modified its information collection protocols of visa applicants. On May 4, 2017, the U.S. Department of State issued a Federal Register Notice under the Paperwork Reduction Act, titled, "Notice of Information Collection Under OMB Emergency Review: Supplemental Question for Visa Applicants."[141] The supplemental request for information from a "subset" of visa applicants included social media handles, aliases, phone numbers, and email addresses over the past five years.[142] The notice purported to request the information as a way to "more rigorously evaluate applicants for terrorism or other national security-related visa ineligibilities[.]"[143] As an emergency action, the notice observed that it would only be in effect for 180 days.[144] On May 18, 2017, a coalition of thirty-five civil and human rights organizations—including the Brennan Center for Justice, Center for Democracy and Technology, EFF, Human Rights Watch, National Immigration Law Center, and others—filed a comment with the U.S. Department of State, expressing concerns that this modification of the protocol, including the collection of social media information, would raise significant constitutional and human rights

138. *See, e.g.*, Hu, *Algorithmic Jim Crow*, *supra* note 135, at 638–43; Hu, *Crimmigration-Counterterrorism*, *supra* note 135, at 984–92.

139. *Ending the Crisis: America's Borders and the Path to Security: Hearing Before the H. Comm. on Homeland Sec.*, 115th Cong. 83 (Feb. 7, 2017), https://docs.house.gov/meetings/HM/HM00/20170207/105474/HHRG-115-HM00-Transcript-20170207.pdf [https://perma.cc/6WAG-WSNU] (statement of John F. Kelly, DHS Secretary). As of the time of publication, the proposal to seek social media passwords have not been officially adopted as a part of official vetting protocol.

140. *See, e.g.*, Hu, *Algorithmic Jim Crow*, *supra* note 135, at 638–43; Hu, *Crimmigration-Counterterrorism*, *supra* note 135, at 984–92.

141. Notice of Information Collection Under OMB Emergency Review: Supplemental Question for Visa Applicants, 82 Fed. Reg. 20,956 (May 4, 2017), https://www.federalregister.gov/documents/2017/05/04/2017-08975/notice-of-information-collection-under-omb-emergency-review-supplemental-questions-for-visa [https://perma.cc/N4F9-9ANS].

142. *Id.*

143. *Id.*

144. *Id.*

concerns.[145] Less than three months later, the State Department issued an additional notice proposing to make the revised collection protocol permanent.[146]

Exactly how DHS intended to use an automated tool for social media vetting gained clarity with media revelations surrounding a DHS "Industry Day," hosted on July 18-19, 2017, to discuss a request for information on an industry contract to build technologies for extreme vetting. During this event, DHS circulated a document entitled: "Extreme Vetting Initiative."[147] This document explained that DHS intended to award contracts to the firms to assist the federal government in counterterrorism-related data analysis.[148] Specifically, through a competitive selection process, contractors would be awarded DHS contracts to fund the collection and analysis of all publicly available social media and online data that is not password protected:

> The contractor shall analyze and apply techniques to exploit publically [sic] available information, such as media, blogs, public hearings, conferences, academic websites, social media websites such as Twitter, Facebook, and LinkedIn, radio, television, press, geospatial sources, internet sites, and specialized publications with intent to extract pertinent information regarding targets, including criminals, fugitives, nonimmigrant violators, and targeted national security threats and their []location.[149]

The "Extreme Vetting Initiative" document asserted that the agency's present capacity to predict a would-be immigrant's potential criminality or terroristic threat level is insufficient as it is "fragmented across mission areas and [is] both time-consuming and manually labor-intensive due to complexities in the current U.S. immigration system."[150]

145. Comment by Coalition of Civil and Human Rights Organizations in Response to 82 Fed. Reg. 20,956 (May 4, 2017) Notice of Information Collection Under OMB Emergency Review: Supplemental Question for Visa Applicants (May 18, 2017), https://www.brennancenter.org/sites/default/files/State%20Dept%20Information%20Collection%20Comments%20-%2051817_3.pdf [https://perma.cc/8J9C-TB78].

146. 60-Day Notice of Proposed Information Collection: Supplemental Question for Visa Applicants, 82 Fed. Reg. 36,180 (Aug. 3, 2017), https://www.federalregister.gov/documents/2017/08/03/2017-16343/60-day-notice-of-proposed-information-collection-supplemental-questions-for-visa-applicants [https://perma.cc/JR53-SCD7].

147. *See id.*

148. *See id.*

149. *Id.*

150. *Id.* (citing DEP'T OF HOMELAND SEC., EXTREME VETTING INITIATIVE STATEMENT OF OBJECTIVES (SOO), http://www.brennancenter.org/sites/default/files/Extreme%20Vetting%20Inititate%20-%20Statement%20of%20Objectives.pdf [https://per ma.cc/F2UW-GWPX]).

ICE stated that it sought a computer-based system that will act as an "overarching vetting" tool "that automates, centralizes, and streamlines the current manual vetting process while simultaneously making determinations via automation if the data retrieved is actionable" in an effort to "implement the President [Donald Trump]'s various Executive Orders (EOs) that address American immigration and border protection security and interests."[151] According to ICE, the ideal system would have the ability to "determine and evaluate an applicant's probability of becoming a positively contributing member of society, as well as their ability to contribute to national interests" and to determine "whether an applicant intends to commit criminal or terrorist acts after entering the United States."[152]

In a follow-up Q&A session with the attendees, DHS conceded that its "biggest constraint, because we are a vetting/screening operation, is that we are required to work with what is publically [sic] available."[153] DHS received a question from an anonymous contractor regarding a potential legal challenge by the American Civil Liberties Union (ACLU).[154] The anonymous question asked:

> Five years ago the FBI tried to accomplish the objectives that are being stated here and the ACLU shut it down. The FBI tried to [do] this type of contract in the past and the ACLU shut them down. Does [DHS] realize the [legal and constitutional] problems of the past and what happened before?[155]

DHS responded that although the FBI had been frustrated in the past while trying to develop a comparable datamining system concentrated on U.S. citizens, the fact that the proposed program would focus on noncitizens and would collect the data on U.S. citizens not on purpose, but incidentally or tangentially, makes it less likely to face such legal hurdles.[156] One official stated: "The prediction is that in the near future there will be legislation

151. Sam Biddle & Spencer Woodman, *These Are The Technology Firms Lining Up To Build Trump's "Extreme Vetting" Program* (Aug. 7, 2017, 12:45 PM), https://theintercept.com/2017/08/07/these-are-the-technology-firms-lining-up-to-build-trumpsextreme-vetting-program/ [https://perma.cc/R2PG-FNM9] (quoting the ICE "Extreme Vetting Initiative" document).

152. *Id.* (quoting the ICE "Extreme Vetting Initiative" document).

153. *Id.* (quoting from a Q&A session between ICE and contractors).

154. *Id.*

155. *Id.*

156. *Id.*

addressing what you can and can't do. . . . We will continue to do it until someone says that we can't."[157]

Shortly thereafter, on September 18, 2017, the DHS Privacy Office introduced a notice under the title of "Notice of Modified Privacy Act System of Records."[158] In the September 2017 DHS Notice, DHS explained that information now would be added to the A-Files[159] of immigrants, including amending its record retention practices to require immigrants to disclose social media accounts. DHS stated that it will now collect information including "social media handles, aliases, associated identifiable information, and search results"[160] on immigrants. This change allows DHS to collect data gathered from Tweets, Facebook posts, Instagram uploads, and other social media search results.

DHS elaborated that the amended practice reflected a policy of "conducting more immigration actions in an electronic environment" that would "[r]edefine which records constitute the official record of an individual's immigration history."[161] This redefinition specifically includes immigrants, lawful permanent residents, and naturalized U.S. citizens' "social media handles, aliases, associated identifiable information, and search results."[162] DHS did not define "search results."

As discussed in Part I, the September 2017 DHS Notice was controversial and generated almost 3,000 comments. Experts note that U.S. citizens who communicate with immigrants would be impacted by the modification to the DHS record system.[163] Other public comments received by DHS question the scientific validity and efficacy of the social media screenings, noting that DHS has not offered any evidence that social media screening thwarts terrorist or criminal risks.[164] Additionally, six U.S.

157. *Id.*

158. Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556 (Dep't of Homeland Sec. Sept. 18, 2017). DHS had previously announced a policy on social media data collection on June 8, 2012. *See supra* note 105 and accompanying discussion in Part II.B. Therefore, it is unclear whether social media data collection was included in the A-File prior to the publication of the "Notice of Modified Privacy Act System of Records" on September 18, 2017.

159. *See supra* note 21.

160. Privacy Act of 1974, 82 Fed. Reg. at 43,556.

161. *Id.*

162. *Id.* at 43,557.

163. *See, e.g.*, *Coalition Letter*, *supra* note 68. *See generally* Comment submitted by Juvaria Khan, Muslim Advocates (Oct. 18, 2017), https://www.muslimadvocates.org/files/MA-Comment-to-DHS-FINAL.pdf [https://perma.cc/WF7W-GSDJ]; Comments submitted by Marc Rotenberg, Jeramie Scott, Christine Bannan, and the Electronic Privacy Information Center (EPIC) (Oct. 24, 2017), https://epic.org/EPIC-DOS-Visas-SocialMediaID-Dec2017.pdf [https://perma.cc/52R9-6R68]; Comments submitted by Marc Rotenberg, Jeramie Scott, Spencer Beall, and the Electronic Privacy Information Center (EPIC) (Sept. 27, 2018), https://epic.org/apa/comments/EPIC-Comments-DOS-Social-Meida-IDs-Sept2018.pdf [https://perma.cc/3VTF-8FU2].

164. *See, e.g.*, *Coalition Letter*, *supra* note 68; Comment submitted by Andrew Sellars, BU/MIT Technology & Cyberlaw Clinic, BU School of Law (Oct. 18, 2018), https://www.regulations.gov/doc

Senators submitted a letter to Acting DHS Secretary, Elaine Duke, posing fifteen questions, seeking additional information on program implementation, and articulating constitutional and privacy concerns.[165]

DHS, in defense of the legality and legitimacy of the September 2017 DHS Notice and the collection of social media data, explained:

> This policy permits . . . USCIS[United States Citizenship and Immigration Services] officers to access publicly available social media as an aid in determining whether an individual is eligible for an immigration benefit. The notice does not authorize USCIS to search the Internet history of these individuals. Furthermore, the notice does not authorize USCIS to search the social media accounts of naturalized citizens; rather, it simply restates USCIS' authority to search publicly available social media information of individuals applying for naturalization and informs the public that this publicly available information will be stored in the applicant's alien file.[166]

On September 24, 2017, President Trump published his third travel ban, a Presidential Proclamation titled "Enhancing Vetting Capabilities and Processes for Detecting Attempted Entry Into the United States by Terrorists or Other Public-Safety Threats."[167] The Proclamation emphasized the need for increased screening and vetting processes, including the collection of biometric and biographic data.[168] The Proclamation followed DHS's September 18, 2017, Federal Register publication of the "Notice of Modified Privacy Act System of Records,"[169] and the CBP's September 21, 2017, "Notice of new Privacy Act System of Records."[170] In October 2017, DHS issued a press release announcing new investigative procedures for refugees from eleven "high-risk" countries that included social media

ument?D=DHS-2017-0038-2960 [https://perma.cc/CCN5-9FGB] [hereinafter Sellars] (discussing overbroad nature of the Notice; concerns about using social media data in a discriminatory manner; effectiveness of social media data collection (e.g., wasting time on fruitless searches, whether terrorists will use hidden accounts, and accuracy of algorithms)); *see also* DHS' PILOTS FOR SOCIAL MEDIA SCREENING, *supra* note 109; SOCIAL MEDIA MONITORING REPORT, *supra* note 1, at 6–7.

165. Sens. Bob Menendez (D-N.J.), Ed Markey (D-Mass.), Patty Murray (D-Wash.), Cory Booker (D-N.J.), Kristen Gillibrand (D-N.Y.), Mazie Hirono (D-Haw.), Letter to Elaine Duke, Acting DHS Secretary (Nov. 20, 2017), https://www.menendez.senate.gov/imo/media/doc/DHS_Social-media-immigration-screening-menendez.pdf [https://perma.cc/8EYJ-DYTB].

166. Novak, *supra* note 27.

167. Proclamation No. 9645, 82 Fed. Reg. 45,161 (Sept. 27, 2017).

168. *Id.* at 45,170.

169. Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556 (Dep't of Homeland Sec. Sept. 18, 2017).

170. Privacy Act of 1974; DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 82 Fed. Reg. 44,198 (Sept. 21, 2017).

checks and an additional ninety-day review period.[171] The enhanced vetting procedures were issued in accordance with Section 6(a) of the second travel ban, Executive Order 13,780.[172] These changes were implemented in January 2018.[173]

On March 30, 2018, the Department of State published two notices in the Federal Register that appear to build upon the social media intelligence gathering efforts: a "Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration,"[174] and a "Notice of Proposed Information Collection: Application for Nonimmigrant Visa."[175] The State Department, Consular Office, in its oversight of the visa application process and in coordination with DHS, has increasingly requested social media account information from visa applicants. Individuals from certain states[176] or who have visited terrorist-controlled areas[177] are required to provide the State Department with all phone number, email, and social media account history for the past five years.[178] Vetting procedures set forth by the State Department as described in the notices have taken effect and include database screening through multiple intelligence agencies, U.S. Department of Defense, and other law enforcement databases

171. *Press Release: Improved Security Procedures for Refugees Entering the United States*, DHS (Oct. 24, 2017), https://www.dhs.gov/news/2017/10/24/improved-security-procedures-refugees-entering-united-states [https://perma.cc/TPN2-9TQ3].

172. *Id.*

173. Laura Koran & Tal Kopan, *US Increases Vetting and Resumes Processing of Refugees from 'High-Risk' Countries*, CNN POLITICS (Jan. 29, 2018, 5:55 PM), https://www.cnn.com/2018/01/29/politics/us-refugee-vetting-measures/index.html [https://perma.cc/DPC7-QJCG].

174. 60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration, 83 Fed. Reg. 13,806 (Dep't of State Mar. 30, 2018).

175. *Id.* at 13,807.

176. *See* Yeganeh Torbati, Mica Rosenberg & Arshad Mohammed, *Exclusive: U.S. Embassies Ordered to Identify Population Groups for Tougher Visa Screening*, REUTERS (March 23, 2017, 5:06 AM), http://www.reuters.com/article/us-usaimmigration-visas-exclusive/exclusive-u-s-embassies-ordered-to-identify-population-groups-for-tougher-visascreening-idUSKBN16U12X [https://perma.cc/6KB8-RVSV]. *But see*, DEP'T OF HOMELAND SEC., CITIZENSHIP LIKELY AN UNRELIABLE INDICATOR OF TERRORIST THREAT TO THE UNITED STATES (Feb. 24, 2017), https://assets.documentcloud.org/documents/3474730/DHS-intelligence-document-on-President-Donald.pdf [https://perma.cc/6MJ6-3VM5] (draft report obtained by Associated Press); Vivian Salama, *AP Exclusive: DHS Report Disputes Threat from Banned Nations*, AP (Feb. 24, 2017), https://apnews.com/39f1f8e4ceed4a30a4570f693291c866 [https://perma.cc/9A4L-BST7].

177. Applicants are asked to provide these details if the officer believes they have "been in an area while the area was under the operational control of a terrorist organization." 60-Day Notice of Proposed Information Collection: Supplemental Questions for Visa Applicants, 82 Fed. Reg. 36,180, 36,181 (Aug. 3, 2017). As the ACLU has pointed out, however, there is no information on how an officer will determine that it "appears" that the applicant was in a region which was under the operational control of a terrorist organization while the applicant was there. American Civil Liberties Union, Comment Letter on Notice of Information Collection under OMB Review 3 (May 18, 2017), https://www.aclu.org/other/aclu-commentsupplemental-questions-visa-applicants [https://perma.cc/5TZ9-PLT6].

178. 82 Fed. Reg. at 36,181.

at the federal and state level.[179]

DHS explains that vetting uses both classified and unclassified databases for biometric and biographic screening, providing corroboration that vetting involves intelligence tools.[180] For example, "refugees' names and biographical information [are checked] against CIA databases[,]"[181] and multiple other databases[182] to automatically screen "cellphone numbers, address books, social media postings, arrest reports and intelligence assessments[.]"[183] DHS specifies that vetting of refugees includes "[a] biometric record check of [the U.S.] Department of Defense (DOD) holdings collected in areas where DOD has or has had a significant military presence."[184]

B. Extreme Vetting Initiative and Visa Lifecyle Vetting Initiative

The Extreme Vetting Initiative appears to build upon the "ICE Investigative Case Management" system (ICM).[185] It is reported that ICM, supported by data analytics company Palantir Technologies through a $41 million contract by DHS, allows for up to "10,000 users" to access up to "tens of millions of subject records."[186] Through multiple databases, both public and private, ICM "can provide ICE agents access to information on

179. *Id.*; *see, e.g.*, Sandra E. Garcia, *U.S. Requiring Social Media Information from Visa Applicants*, N.Y. TIMES (June 2, 2019), https://www.nytimes.com/2019/06/02/us/us-visa-application-social-media.html [https://perma.cc/H3LX-UE65]; Faiza Patel, *Stop Collecting Immigrants' Social Media*, N.Y. TIMES (June 30, 2019), https://www.nytimes.com/2019/06/30/opinion/immigrants-social-media.html.

180. DEP'T HOMELAND SEC., U.S. CITIZENSHIP & IMMIGR. SERVS., REFUGEE SECURITY SCREENING FACT SHEET 6 (Aug 28, 2018), https://www.uscis.gov/sites/default/files/USCIS/Refugee%2C%20Asylum%2C%20and%20Int%27l%20Ops/Refugee_Screening_and_Vetting_Fact_Sheet.pdf [https://perma.cc/A4PR-NK5X] [hereinafter DHS REFUGEE SECURITY SCREENING FACT SHEET] ("CBP's [DHS Customs and Border Protection] National Targeting Center-Passenger conducts biographic vetting of all ABIS biometric matches (both derogatory and benign) against various classified and unclassified U.S. government databases.").

181. Del Quentin Wilber & Brian Bennett, *Federal Agents Are Reinvestigating Syrian Refugees in U.S. Who May Have Slipped Through Vetting Lapse*, L.A. TIMES (Jan. 25, 2017, 9:55 AM), https://www.latimes.com/politics/la-na-syria-refugees-vetting-gap-20170125-story.html [https://perma. cc/33FU-BGSX].

182. *Id.* (databases include those of DHS, Department of State, CIA, FBI, and National Counterterrorism Center, and Department of Defense).

183. *Id.*

184. DHS REFUGEE SECURITY SCREENING FACT SHEET, *supra* note 180, at 6 ("DOD screening began in 2007 for Iraqi applicants and incrementally expanded to all refugee nationalities by 2013.").

185. *See* Spencer Woodman, *Palantir Provides the Engine for Donald Trump's Deportation Machine*, INTERCEPT (Mar. 2, 2017, 12:18 PM), https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/ [https://perma.cc/ESQ4-LARN] (DHS granted Palantir a $41 million contract in 2014 to build ICM, a "vast 'ecosystem' of data" to assist ICE agents in discovering potential deportation cases through access to multiple intelligence databases managed by several agencies).

186. *Id.*

a subject's schooling, family relationships, employment information, phone records, immigration history, foreign exchange program status, personal connections, biometric traits, criminal records, and home and work addresses."[187] ICM is reported to be reliant upon two intelligence data systems: ICE's FALCON and the CBP's Analytical Framework for Intelligence (AFI).[188] FALCON, a data mining and data analytic network, allows DHS Office of Homeland Security Investigations agents to track immigrants and conduct data analysis on cross-border crimes.[189] ICM also grants its users access to AFI, a largely classified database.[190] Experts have speculated that the risk assessment profiling algorithms associated with "extreme vetting" are intended to be built upon the algorithms of AFI.[191] "'When Trump uses the term 'extreme vetting[,]' AFI is the black-box system of profiling algorithms that he's talking about. This is what extreme vetting means.'"[192]

DHS announced that the "Extreme Vetting" Initiative had been renamed the "Visa Lifecycle Vetting Initiative."[193] On February 6, 2018, the White House released "Presidential Memorandum on Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise."[194] The Memorandum announced the creation of a National Vetting Center to coordinate the use of intelligence and other information among all executive departments and agencies that will be run by the "Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence, and

187. *Id*.

188. *Id*. (citing OFFICE OF THE CHIEF INFORMATION OFFICER, REPLAN 04152014, ICE TECS MODERNIZATION PROGRAM TEST AND EVALUATION MASTER PLAN (Apr. 2, 2014), https://assets.documentcloud.org/documents/3478488/ICE-TECS-Modernization-Master-Plan.pdf [https://perma.cc/CBN4-JN46]).

189. *Id.*

190. *Id.*; *see also* U.S. DEP'T HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR THE ANALYTICAL FRAMEWORK INTELLIGENCE (AFI) DHS/CBP/PIA-010(a) (Sept. 1, 2016, appendix updated Mar. 2019), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-010-a-afi-2016.pdf [https://perma.cc/LF2H-GRDA] [hereinafter DHS PIA AFI]; *infra* Part IV.B.1 (citing AFI Use in DHS Notice, Titled, Privacy Act of 1974; DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 82 Fed. Reg. 44,198 (Sept. 21, 2017)).

191. Woodman, *supra* note 185.

192. *Id.* (quoting Edward Hasbrouck, Identity Project).

193. *See, e.g.*, Faiza Patel and Harsha Panduranga*, DHS' Constant Vetting Initiative: A Muslim-Ban by Algorithm*, JUSTSECURITY (Mar. 12, 2018), https://www.justsecurity.org/53671/dhs-constant-vetting-initiative-muslim-ban-algorithm/ [https://perma.cc/H49Y-AWFL]; *see also* Chinmayi Sharma, *The National Vetting Enterprise: Artificial Intelligence and Immigration Enforcement*, LAWFARE (Jan. 8, 2019), https://www.lawfareblog.com/national-vetting-enterprise-artificial-intelligence-and-immigration-enforcement [https://perma.c c/G78S-WUHS].

194. *Memorandum on Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise*, 2018 DAILY COMP. PRES. DOC. 79 (Feb. 6, 2018), https://www.govinfo.gov/content/pkg/DCPD-201800078/pdf/DCPD-201800078.pdf [https://perma.cc/LL8W-JYZ3].

the Director of the Central Intelligence Agency[.]"[195] The memo seeks "contextual information" in addition to "biographic" and "biometric" information.[196]

By May 2018, ICE spokeswoman Carissa Cutrell explained that the Visa Lifecycle Vetting Initiative program had "'shifted from a technology-based contract to a labor contract.'"[197] In other words, this DHS statement is intended to suggest that ICE is moving away from an algorithmic-based technology where the data analysis is automated and has, instead, made the decision to move to a human-based "labor contract" to analyze the data.[198] Cutrell explained that ICE's Counterterrorism and Criminal Exploitation Unit receives "1.2 million 'investigative leads' per year" and prioritizes how to address the investigative lead through an assessment of threat.[199] Yet, DHS had previously announced that it was pursuing an automated, algorithmic-based tool to assist in assessing risk because it was "believed an automated system would provide a more effective way to continuously monitor the 10,000 people determined to be the greatest potential risk to national security and public safety."[200]

Cutrell explained that, through the Visa Lifecycle Vetting Initiative, ICE sought continuous monitoring of social media behavior to detect "radical or extremist views."[201] ICE's Acting Director, Thomas Homan, explained that enhanced analytical tools utilized social media data.[202] Homan stated that senior analysts reviewed the leads generated from these tools before the leads were used in investigations.[203]

"Contract-request documents in June 2017 said the automated system should contribute to its agents' work and 'generate a minimum of 10,000 investigative leads annually.'"[204] Under revisions to the Visa Lifecycle Vetting Initiative contract, DHS explained that, rather than seek a quota of 10,000 investigative leads annually, it would request that the contractor be required to employ "180 people to monitor the social-media posts of those 10,000 foreign visitors whom ICE flagged as high-risk, generating new

195. *Id.* at 2.
196. *Id.* at 1.
197. Drew Harwell & Nick Miroff, *ICE Just Abandoned its Dream of 'Extreme Vetting' Software that Could Predict Whether a Foreign Visitor Would Become a Terrorist*, WASH. POST (May 17, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/ [https://perma.cc/83MU-TZAN].
198. *Id.*
199. *Id.*
200. *Id.*
201. *Id.*
202. *Id.*
203. *Id.*
204. *Id.*

leads as they keep tabs on their social-media use."[205]

On June 4, 2018, DHS issued a Request for Quotation (RFQ) through the General Services Administration (GSA), seeking bids from potential vendors by July 11, 2018.[206] The RFQ explained that the vendors would be asked to provide operations support services to the Visa Security Program (VSP) and the Counterterrorism and Criminal Exploitation Unit (CTCEU) within DHS's Visa Lifecycle Vetting Initiative.[207] After an initial evaluation, SRA, later named CSRA and then acquired by General Dynamics,[208] was awarded a contract from DHS for approximately $113 million.[209] After reviewing bid protests by competing vendors, on April 9, 2019, the General Counsel of the U.S. Government Accountability Office (GAO) reaffirmed GSA's decision to grant CSRA a five-and-one-half-year blanket purchase agreement to support the Visa Lifecycle Vetting Initiative.[210] CSRA has reportedly employed approximately one-hundred human analysts to fulfill this contract.[211]

Because DHS social media data collection appears to contribute to preexisting data intelligence structures, such as the FALCON and AFI systems described above, it is unclear whether the data analysis will be human labor-focused, as presented by DHS spokespersons, or algorithmic-focused, as was previously represented by DHS. For example, shortly after the DHS RFQ was issued by GSA in June 2018 to secure a vendor for the Visa Lifecycle Vetting Initiative, DHS secured the services of Giant Oak, Inc. for "open source/social media data analytics."[212] In August 2018, Giant Oak received contracts to support the DHS Visa Security Program and CTCEU,[213] and in September 2018, it was contracted to support ICE.[214] It

205. *Id.*

206. *In re* ManTech Adv. Sys. Int'l, Inc., No. B-416734 (U.S. Gov. Accountability Office Nov. 27, 2018).

207. *Id.*

208. *General Dynamics Completes Acquisition of CSRA*, GENERAL DYNAMICS (Apr. 2, 2018), https://www.gd.com/en/Articles/2018/04/02/general-dynamics-completes-acquisition-csra [https://perma.cc/YP8R-KVDQ].

209. *In re* ManTech Adv. Sys. Int'l, Inc., No. B-416734.

210. *See In re* Amyx, Inc., No. B-416734.2 (U.S. Gov. Accountability Office Apr. 9, 2019) ("The RFQ contemplated the issuance of a fixed-price BPA to be performed over a 1-year base period, four 1-year option periods, and one 6-month extension period.") (internal citations omitted).

211. McKenzie Funk, *How ICE Picks its Targets in the Surveillance Age*, N.Y. TIMES (Oct. 3, 2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.

212. SOCIAL MEDIA MONITORING REPORT, *supra* note 1, at 25.

213. *Id.* at n.353 (citing *Open Source/Social Media Data Analytics—VSP: Aug. 21, 2018–Aug. 20, 2019*, USA SPENDING, https://www.usaspending.gov/#/award/67807277 [https://perma.cc/EJW9-MLHR]; *Open Source/Social Media Data Analytics—CTCEU: June 13, 2018–Aug. 31, 2019*, USA SPENDING, https://www.usaspending.gov/#/award/66685141 [https://perma.cc/WJQ4-JWQ9]).

214. *Id.* at nn.354–55 (citing *Spending by Prime Award: Sept. 4, 2014–Sept. 24, 2018*, USA SPENDING, https://www.usaspending.gov/#/search/f2b8f8d69d8696753510a172f52d46ad [https://perma.cc/P8RH-8MTZ]; *Open Source/Social Media Data Analytics for CBP: Sept. 24, 2018–*

is not fully known how data is collected and analyzed by DHS vendors such as Palantir, CSRA, Great Oak, and others.

The discussion below in Part IV explores how the September 2017 DHS Notice suggests that the social media data collection can be used to create new intelligence products through database screening, algorithmic-based tools and data analytics, and artificial intelligence. It focuses especially on the integrated data environment of the AFI system. The discussion assists in better understanding why DHS social media data collection should not be simply characterized as a record-keeping action under DHS's system of records that falls within the Privacy Act. But, rather, DHS social media data collection should be more accurately classified as a surveillance program that necessitates independent authorization by Congress.

IV. PRIVACY AND TRUST: DISTRUST IN THE PRIVACY ACT

This Part aims to help illuminate the potential legal challenges that accompany the implementation of social media surveillance programs through administrative means, such as Federal Register Notices published pursuant to the Privacy Act, rather than through congressionally approved data collection and intelligence gathering programs. To help explain this impact, the discussion below specifically focuses on why the implementation of reporting requirements under the Privacy Act by DHS seems ironic. Part A provides a general discussion of the provisions of the Privacy Act that merit close inspection in the September 2017 DHS Notice. Without a close inspection of these provisions, it would be impossible to understand the privacy law impact of the Notice. In Part B, the discussion specifically focuses on how this Notice is a part of a trajectory of reliance upon the law enforcement exemptions of the Privacy Act by DHS in other post-9/11 Privacy Act Notices.

A. Examining Methods of Subverting the Privacy Act's Intent: DHS Notice "Privacy Act of 1974; System of Records" (September 18, 2017)

The Privacy Act requires that federal agencies give the public notice of "systems of records" and modifications to federal systems of records through publication in the Federal Register, often referred to as a SORN (System of Records Notice published in the Federal Register Notice under

Sept. 24, 2019, USA SPENDING, https://www.usaspending.gov/#/award/68790969 [https://perma.cc/6A74-CPH9]; *Open Source/Social Media Data Analytics: Sept. 25, 2017–Aug. 31, 2022*, USA SPENDING, https:// www.usaspending.gov/#/award/23831407 [https://perma.cc/YE28-XPXK]; Statement of Work, ICE Contract #HSCEMD-14-C-00002 P00007, 31).

the Privacy Act of 1974),[215] as discussed above. The September 2017 DHS Notice conforms to the Act's specific mandate that a federal agency publicly disclose modifications to its record-keeping practices. The "Background" discussion of the Notice states that "DHS is updating" the following system of records held by DHS: "DHS/USCIS [U.S. Citizenship and Immigration Services]/ICE [U.S. Immigration and Customs Enforcement]/CBP [U.S. Customs and Border Protection]-001 Alien File, Index, and National File Tracking System of Records."[216] In the updating of the A-File system of records, DHS explained that it would promulgate twelve separate "substantive changes[.]"[217] Some "substantive changes" involve clarifying

215. 5 U.S.C. § 552a(e)(4).

216. Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556, 43,557 (Dep't of Homeland Sec. Sept. 18, 2017).

217. *Id.* at 43,557–58. In the Notice Background, DHS explains that it "is updating" the A-File system of records to include "substantive changes" in the following twelve instances:

> (1) Redefine which records constitute the official record of an individual's immigration history to include the following materials and formats: (a) The paper A-File, (b) the electronic A-File, or (c) a combination of paper and electronic records and supporting documentation;
>
> (2) clarify that data originating from this system of records may be stored in a classified paper A-File or classified electronic network;
>
> (3) provide updated system locations;
>
> (4) update category of individuals covered by this SORN to include individual acting as legal guardians or designated representatives in immigration proceedings involving individuals who are physically or developmentally disabled or severely mentally impaired (when authorized); Civil Surgeons who conduct and certify medical examinations for immigration benefits; and law enforcement officers who certify a benefit requestors cooperation in the investigation or prosecution of a criminal activity; and interpreters;
>
> (5) expand the categories of records to include country of nationality; country of residence; the USCIS Online Account Number; social media handles, aliases, associated identifiable information, and search results; and information regarding the DOJ Executive Office for Immigration Review (EOIR) and BIA proceedings;
>
> (6) add and describe the purpose of the USCIS ELIS, EDMS, and Microfilm Digitization Application System (MiDAS);
>
> (7) expand data elements used to retrieve records;
>
> (8) update the parameters for retention and disposal of paper A-Files and electronic A-Files;
>
> (9) include the MiDAS retention schedule;
>
> (10) change system manager to Associate Director, Immigration Records and Identity Services (IRIS);
>
> (11) update record source categories to include publicly available information obtained from the internet, public records, public institutions, interviews, commercial data providers, and information shared obtained through information sharing agreements; and
>
> (12) update routine use E to comply with Office of Management and Budget Circular A-108.

Id.

data storage and where the system is located.[218] Other "substantive changes" raise potential constitutional and legal issues.[219] As a result of the "substantive changes," the September 2017 DHS Notice impacted the system of records—"DHS/USCIS/ICE/CBP001 Alien File, Index, and National File Tracking System of Records"—in the following ways: (1) the types and sources of data collected, and the categories of individuals whose data is collected; (2) the conditions of disclosure, including the characterization of the "routine uses"[220] of the system of records; and (3) the exemptions claimed under the Privacy Act.[221] Each one of these will be discussed below. The purpose of this description is to help examine how what DHS has presented as an update to the system of records in fact subverts the intent of the Privacy Act.

1. Sources and Types of Information Collected, and Categories of Individuals

a. Categories of Records and Sources of Information

One of the "substantive changes" in the September 2017 DHS Notice is an "expan[sion of] the categories of records."[222] The Privacy Act states that when there is a "revision" of a system of records, the notice shall include the "categories of records maintained in the system."[223] Under the Privacy Act, the required notice to a revision of a system of records must also include the "categories of sources" for the system.[224] The September 2017 DHS Notice explains that DHS collects data from multiple sources:

> Basic information contained in DHS records is supplied by individuals on Department of State (DOS) and DHS applications and forms. Other information comes from publicly available information obtained from the Internet, public records, public institutions, interviewees, commercial data aggregators, inquiries or complaints from members of the general public and members of Congress, referrals of inquiries or complaints directed to the President or Secretary of Homeland Security, information shared

218. *Id*. at 43,557 (referring to "substantive changes" in the instances of (2) (data storage) and (3) (system location)).

219. *See supra* notes 67–74; *see infra* Conclusion.

220. *See* § 552a(a)(7) ("The term 'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected").

221. Privacy Act of 1974, 82 Fed. Reg. at 43,556.

222. *Id.* at 43,557.

223. § 552a(e)(4)(C).

224. § 552a(e)(4)(I).

> through information sharing agreements, reports of investigations, sworn statements, correspondence, official reports, memoranda, and written referrals from other entities, including federal, state, and local governments, various courts and regulatory agencies, foreign government agencies, and international organizations. [225]

The Notice updates the list of sources DHS is allowed to gather personal information from to include: "publicly available information obtained from the internet, public records, public institutions, interviews, commercial data providers, and information shared or obtained through information sharing agreement."[226] It is unclear how these sources will be used or what the impact will be.

As discussed above, the Notice broadens the categories of information collected to include "social media handles, aliases, associated identifiable information, and search results."[227] However, as one commenter points out "'social media' is not defined, and could be broadly interpreted to include any online platform or site that enables users to publicly post content, communicate with each other, or communicate with the operator or host."[228] This ambiguity makes it impossible to fully understand the impact of the changes proposed in the Notice.

Multiple commenters have expressed concern that the deployment of algorithmic decisionmaking by DHS changes the nature of the system of records.[229] In fact, it is an open question whether the new volume of data reflected by the collection of social media data can be correctly characterized as a "modification" of a system of records. The Notice does not answer whether the social media data will be reconfigured into new intelligence products or new forms of knowledge, for example, through predictive analytics and artificial intelligence.[230] In a separate DHS Federal Register Notice, published on September 21, 2017, titled, "Privacy Act of 1974; DHS/CBP-024 Intelligence Records System (CIRS) System of Records," DHS explains that commonalities in data patterns can form the foundation for new intelligence products: "These commonalities can also form the basis for a DHS-generated intelligence product that may lead to further investigation or other appropriate follow-up action by CBP, DHS,

225. Privacy Act of 1974, 82 Fed. Reg. at 43,561.
226. *Id.* at 43,558.
227. *Id.* at 43,557.
228. *Coalition Letter*, *supra* note 68.
229. *See* Sharma, *supra* note 193; Patel & Panduranga, *supra* note 193; *Coalition Letter*, *supra* note 68; Duarte, *supra* note 71; Rotenberg & Scott, *supra* note 69; Sellars, *supra* note 164.
230. *See* Biddle & Woodman, *supra* note 151; Woodman, *supra* note 185 (quoting Edward Hasbrouck, Identity Project, explaining that, "AFI is the black-box system of profiling algorithms[.]").

or other federal, state, or local agencies."[231]

In a Privacy Impact Assessment published by DHS on September 1, 2016, DHS provides important information on the integrated data intelligence structure for the Analytical Framework for Intelligence (AFI) system.[232] AFI provides insight into why social media data is considered critical to DHS intelligence operations: "AFI permits certain AFI users to upload and store information that may be relevant from other sources, such as the Internet (including social media) or traditional news media, into projects or final intelligence products."[233]

The AFI system operates efficiently by using data from multiple systems of records.[234] DHS explains that, "AFI is specifically designed to make the intelligence research and analysis process more efficient by allowing searches of a broad range of data through a single interface. AFI can also identify links (relationships) between individuals or entities based on commonalities, such as identification numbers, addresses, or other information."[235]

Through the publication of a March 2019 update to the AFI Privacy Impact Assessment,[236] DHS provided two appendices: Appendix A,[237] "Approved AFI External Users (non-CBP Users)," and Appendix B,[238] "List of relevant Systems and SORNS, where applicable, for data available through AFI." In Appendix A, DHS explains that although AFI was originally developed to support border security by CBP, the use "has expanded to allow access" to other DHS intelligence programs.[239] In Appendix B, DHS states CBP-related data in AFI's associated system of records and other system interfaces includes twenty-six additional

231. Privacy Act of 1974; DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 82 Fed. Reg. 44,198, 44,199 (Sept. 21, 2017) ("These commonalities in and of themselves are not suspicious, but in the context of additional information they sometimes help DHS agents and analysts to identify potentially criminal activity and identify other suspicious activities.").

232. DHS PIA AFI, *supra* note 190.

233. *Id.* at 4; *see also id.* at n.19 ("*See* DHS/CPB-017 Analytical Framework for Intelligence System, June 7, 2012, 77 FR 13813, which 'permits analysts to upload and store any information from any source including public and commercial sources, which may be relevant to projects, responses to RFIs, or final intelligence products.'").

234. *See id.* at 1.

235. Privacy Act of 1974, 82 Fed. Reg. at 44,199.

236. DHS PIA AFI, *supra* note 190 (announcing March 2019 update on DHS website).

237. *Id.* at 20–22.

238. *Id.* at 23–29.

239. *Id.* at 20–22. (Non-CBP users of AFI now include USCIS: Fraud Detection and National Security Directorate (FDNS); ICE: Homeland Security Investigations Office of Intelligence; Transportation Security Administration (TSA): Office of Intelligence and Analysis; U.S. Coast Guard (USCG): Office of Intelligence; DHS Office of Intelligence and Analysis; USCIS: Background Check Units (BCUs) and Security Vetting and Program Integrity Branch (SVPI); DHS Office of the Chief Security Officer (OCSO); U.S. Secret Service: Global Investigative Operations Center.).

systems.[240] Appendix B further elaborates that the "AFI and CIRS" (CPB Intelligence Records System) system of records include an additional fifteen systems and databases that are ICE-affiliated;[241] five systems and databases that are USCIS-affiliated;[242] one system that is TSA-affiliated;[243] one system that is Cybersecurity and Infrastructure Security Agency (CISA);[244] and ten other systems that are inclusive of other governmental or commercial data.[245]

AFI and social media data collection that facilitates automated database matching to identify individuals appear to implicate the justification for the

240. *Id.* at 23–25 (CBP-related data in AFI's associated system of records and other system interfaces include: Advanced Passenger Information System (APIS); Intelligence Reporting System (IRS-NG); Centers of Excellence and Expertise (CEE) import data; Currency or Monetary Instrument Reports (CMIR); Electronic System for Travel Authorization (ESTA); Electronic Export Information; I 94-Arrival and Departure Records; TECS [formerly known as the Treasury Enforcement Communications System] IO04 Land Border Secondary; TECS IO25 Airport Secondary; IECS IOIL Incident Log; TECS Primary Crossing Person (Primary Query); IECS Primary Crossing Vehicle; TECS Business Subject Records; TECS-Memoranda of Information Received (MOIRs); TECS-Person Subject Records; TECS-Vehicle Subject Records; TECS Reports of Investigation; Seized Assets and Case Tracking System-Arrest Seizure Incidents; Arrival and Departure Information System (ADIS); Customs-Trade Partnership Against Terrorism (C-TPAT); Electronic Visa Update System (EVUS); Global Enrollment System (GES); Port Radiation Inspection, Detection & Evaluation (PRIDE); Automated Targeting System-Passenger Name Record (PNR); Document and Media Exploitation (DOMEX); Agriculture Programs Trade Liaison (APTL)) (internal citations omitted).

241. *Id.* at 25–26 (databases affiliated with ICE that "enable CBP's collection of this information" under AFI and CIRS include: Enforcement Integrated Database-Civilian Detention Data; Enforcement Integrated Database-I213, Record of Deportable-Inadmissible Alien; Enforcement Integrated Database-Incidents; Enforcement Integrated Database-Apprehension (Deprecated); Enforcement Integrated Database-Detention (Deprecating); Enforcement Integrated Database-Inadmissible (Deprecating); Enforcement Integrated Database-Seizures (Deprecating); Detention and Removal Operations-LEAD Report; Legacy ICE Intelligence Information Reports; Finished ICE Intelligence Products; Legacy ICE NameTrace; Legacy National Security Entry Exit Registration System (NSEERS); Student and Exchange Visitor Information (SEVIS)-Exchange; Student and Exchange Visitor Information (SEVIS)-Student; Biometric Identification Transnational Migration Alert Program (BITMAP)) (internal citation omitted).

242. *Id.* at 26 (databases affiliated with USCIS include: Central Index System (CIS); Computer Linked Application Information Management System (CLAIMS 3); Computer Linked Application Information Management System (CLAIMS 4); Customer Profile Management System (CPMS); and National File Tracking System (NFTO)).

243. *Id.* (a database affiliated with TSA includes Secure Flight Passenger Data (SFPB)).

244. *Id.* at 26–27 (a database affiliated with CISA includes Automated Biometric Identification System (IDENT)).

245. *Id.* at 27–29 (databases associated with other governmental and commercial data includes: U.S. Department of State Consular Electronic Application Center (CEAC); U.S. Department of State Personal Identification Secure Comparison and Evaluation System (PISCES); U.S. Department of State Consular Consolidated Database (CCD); Homeland Security Law Enforcement Information Sharing Service (LEIS)-State and Local Criminal Justice Information Services (CJIS); Homeland Security Law Enforcement Information Sharing Service-National Data Exchange (N-DEx); FBI National Crime Information Center (NCIC); DOS [U.S. Department of State]/DOC [U.S. Department of Commerce]/Treasury Consolidated Screening List; National Law Enforcement Telecommunication System (NLETS) Driver; National Law Enforcement Telecommunication System (NLETS) Vehicle; Canadian National Law Enforcement Telecommunication System (NLETS)); *see also* SOCIAL MEDIA MONITORING REPORT, *supra* note 1, at 35–36.

CMPPA (Computer Matching Privacy Protection Act of 1988) that amended the Privacy Act of 1974. The CMPPA was enacted to address "large numbers of individuals [that] were subjected to automated scrutiny with potentially adverse consequences, and that in actual practice, that meant automated comparisons of automated data bases . . . [and] that use of computers could 'greatly magnify the harm' to an individual."[246] However, CMPPA does not include "matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws[.]"[247] Here, at least one commenter has questioned whether criminal law enforcement is at the center of the A-File System of Records or whether the A-File System of Records is predominantly a record system that serves civil law purposes (e.g., adjudication of immigration benefits and immigration status).[248]

The CMPPA is limited in its reach.[249] The Federal Register Notice

246. Privacy Act of 1974; Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25,818 (Office of Mgmt. & Budget June 19, 1989).

247. 5 U.S.C. § 552a(a)(8)(B)(iii). The Privacy Act defines the term "matching program" as including a "computerized comparison" of:

> (i) two or more automated systems of records or a system of records with non-Federal records for the purpose of--
>
> > (I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or
> >
> > (II) recouping payments or delinquent debts under such Federal benefit programs, or
>
> (ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records[.]

§ 552a(a)(8)(A)(i-ii).

248. *See, e.g.*, NEILSON, *supra* note 62, at 5.

249. The Privacy Act states that the definition of the term "matching program" does not include matches cited:

> (i) . . . to produce aggregate statistical data without any personal identifiers;
> (ii) . . . to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals;
> (iii) . . . by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons;
> (iv) matches of tax information . . .[;]
> (v) matches--
>
> > (I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes . . .; or
> >
> > (II) conducted by an agency using only records from systems of records maintained by that agency;

published on June 19, 1989, promulgating Final Guidance in the implementation of CMPPA, explained that: "It should be noted that the four elements, (i.e., computerized comparison, categories of subjects, Federal benefit program, and matching purpose) all must be present before a matching program is covered under the provisions of the Computer Matching [and Privacy Protection] Act [of 1988]."[250] It could be argued by DHS that the issues raised by the commenters in response to the DHS Federal Register Notice, "Privacy Act of 1974; System of Records," published on September 18, 2017, fall outside of the scope of the CMPPA because DHS will likely argue that the data collection serves both criminal law enforcement purposes and counterterrorism objectives, and because DHS could contend that the four elements are not satisfied.[251]

b. Categories of Individuals

Pursuant to the Privacy Act, when an agency establishes or revises a system of records, it is required to publish a notice in the Federal Register detailing the categories of individuals whose information will be stored in the system of records.[252] The September 2017 DHS Notice introduces four new categories of individuals covered by the system: legal guardians, representatives of the physically or developmentally disabled or mentally impaired, civil surgeons, and law enforcement officers who certify

> if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel;
> (vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel;
> (vii) matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986;
> (viii) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. 402(x)(3), 1382(e)(1));
> (ix) matches performed by the Secretary of Health and Human Services or the Inspector General of the Department of Health and Human Services with respect to potential fraud, waste, and abuse, including matches of a system of records with non-Federal records; or
> (x) matches performed pursuant to section 3(d)(4) of the Achieving a Better Life Experience Act of 2014[.]

§ 552a(a)(8)(B)(i-x) (internal citation omitted).

250. Privacy Act of 1974; Final Guidance Interpreting the CMPPA, 54 Fed. Reg. at 25,823.

251. In the final guidance for the CMPPA, the Office of Management and Budget explained that commenters were concerned that federal agencies may attempt to subvert the intent of the Act. *See, e.g.*, *id.* at 25,818 (noting that commenters expressed concern that federal agencies may engage in "sophistry or subterfuge, to avoid the reach of the Act. . . . [A] Federal agency might combine two disparate systems of records . . . into a single system and match data sets within the new system. This activity would not be covered[.]").

252. § 552a(e)(4)(B).

requestor cooperation.[253] The Notice does not make clear to what extent the social media of these individuals will be monitored, leaving open the possibility that data such as "family history, medical information, and the fruits of social media searches" on the newly covered categories of individuals will be collected.[254]

2. Conditions of Disclosure and "Routine Uses"

Generally, federal agencies that hold a system of records are prohibited from disclosing the information to other agencies and other entities "except pursuant to a written request by, or with the prior consent of, the individual to whom the record pertains," unless the federal agency can claim that the disclosure of the record meets certain "conditions of disclosure."[255] One of

253. *See, e.g.*, Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556, 43,559 (Dep't of Homeland Sec. Sept. 18, 2017).

254. NEILSON, *supra* note 62, at 4.

255. § 552a(b):

> Conditions of disclosure.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—
>
> (1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
>
> (2) required under section 552 of this title;
>
> (3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;
>
> (4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;
>
> (5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
>
> (6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;
>
> (7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
>
> (8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
>
> (9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
>
> (10) to the Comptroller General, or any of his authorized representatives, in the

the conditions of disclosure is a "routine use" of the record.[256] The Privacy Act states that proper notice "shall include. . . each routine use of the records contained in the system, including the categories of users and the purpose of such use."[257]

The September 2017 DHS Notice additionally states that several modifications to the databases fall within "routine uses[,]"[258] yet, the Notice does not specify precisely the nature of the modifications.[259] Under the Privacy Act, the government may disclose to other individuals or agencies the information it has stored on an individual without the individual's consent when the sharing of that information conforms to "routine use," one of the statutory conditions of disclosure.[260] The "routine use" condition of disclosure under the Privacy Act can allow for a broad expansion over time of the entities to which an individual's collected records may be disclosed.[261]

The Notice further specifies that "[a] notice detailing this system of records was last published in the Federal Register on November 21, 2013, as the DHS/USCIS/ICE/CBP001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864." The September 2017 DHS Notice states that routine use E has been updated to comply with a new policy set forth by the Office of Management and Budget (OMB).[262] The Notice does not specify what revisions were made but did provide an updated list of all routine uses pursuant to the Privacy Act.[263] In contrast, the previous time DHS modified the routine uses of the system of records in 2013, DHS specified that it had added five new uses, modified eight more, and provided a summary of what changes were being made and why they were being made. [264]

---

course of the performance of the duties of the Government Accountability Office;

(11) pursuant to the order of a court of competent jurisdiction; or

(12) to a consumer reporting agency in accordance with section 3711(e) of title 31.

Id.

256. § 552a(b)(3).

257. § 552a(e)(4)(D).

258. Privacy Act of 1974, 82 Fed. Reg. at 43,556.

259. *See* NEILSON, *supra* note 62, at 3.

260. § 552a(b)(3).

261. *The Privacy Act of 1974*, EPIC, https://epic.org/privacy/1974act/ [https://perma.cc/6TXV-Q2XH].

262. Privacy of 1974, 82 Fed. Reg. at 43,556 (identifying substantive changes to G and K).

263. § 552a-(e)(4)(D).

264. *Compare* Privacy Act of 1974, 82 Fed. Reg. at 43,556, *with* Privacy Act of 1974; Department of Homeland Security U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection—001 Alien File, Index, and National File Tracking System of Records, 78 Fed. Reg. 69,864 (Nov. 21, 2013).

3. Exemptions

As discussed above, conditions of disclosure under the Privacy Act describe certain conditions present for DHS to legally disclose information to others—including other federal agencies, contractors, and other private individuals.[265] Unlike conditions of disclosure, certain Privacy Act exemptions allow federal agencies to prevent an individual from being able to access the records that the agency possesses on him or her.[266] Some of the exemptions operate to prevent individuals from accessing records held about them by, for example, denying an individual's request "to gain access to his record or to any information pertaining to him which is contained in the system [of records]" and exempting the agency from "establish[ing] procedures whereby an individual can be notified in response to his request[.]"[267]

The Privacy Act exemptions are divided into two categories. The first category is characterized as "[g]eneral exemptions,"[268] and includes a law enforcement exemption.[269] The second category pertains to "[s]pecific

265. *See, e.g.*, § 552a(b)(1)–(12).

266. *See, e.g.*, §§ 552a(d)(5), (j)(1)–(2), (k)(1)–(7).

267. DHS claims it is exempt from § 552a(d) ("Access to records.—Each agency that maintains a system of records shall—(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system[]") and § 552a(f):

> (f) Agency rules.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—
>
> (1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him[.]

Id.

268. § 552a(j).

269. § 552a(j)(2). A system of record held by a federal agency is exempted under the Law Enforcement "General Exemptions" if the record system is:

> (j) General exemptions.—
>
> (2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision. At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

exemptions."[270] Here, the September 2017 DHS Notice specifically claims exemptions under both.

In the September 2017 DHS Notice, DHS exempts the system of records from multiple provisions of the Privacy Act pursuant to the "general exemption" allowed for law enforcement purposes under 5 U.S.C. § 552a(j)(2).[271] The law enforcement exemption allows for the agency under subsection (j)(2) to exempt systems of records from certain provisions of the Privacy Act when the system of records pertains to an agency or component of an agency whose "principal function" is the enforcement of criminal laws.[272] Furthermore, for the law enforcement exemption to apply, the information collected must pertain to identifying an offender or suspected offender, and the data must, in some way, relate to furthering some stage of criminal law enforcement: investigation, arrest, prosecution, parole, etc.[273] The Notice states that when DHS receives a record from another source system, and the system is covered by the law enforcement exemption, DHS will claim the same exemption.[274] Further, the Notice states that DHS will also claim any additional exemptions that are attached to the original system of records.[275]

DHS also claims "specific exemptions" under subsections (k)(1) and (k)(2).[276] The Privacy Act's specific exemptions under 5 U.S.C. § 552a(k)(1) and (k)(2) allow the head of a federal agency to promulgate rules of exemption from any system of records held by the agency under certain

Id.

270. § 552a(k).

271. "The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act pursuant to § 552a(j)(2): 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (e)(12), (f), (g)(1), and (h)." Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556, 43,564 (Dep't of Homeland Sec. Sept. 18, 2017); *see also* Appendix B.

272. § 552a(j)(2).

273. *Id.*

274. Privacy Act of 1974, 82 Fed. Reg. at 43,564 ("When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.").

275. *Id.*

276. *Id.* ("Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2): 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f)[]"); *see also* Appendix C.

provisions.[277] The exemption that DHS claims under (k)(1)[278] relates to 5 U.S.C. § 552(b)(1), allowing an agency to withhold records when the information is related to national defense or foreign policy interests and has been classified by Executive Order.[279] The specific exemption under (k)(2) allows an agency to withhold information it has collected on an individual for law enforcement purposes that are outside the scope of subsection (j)(2); however, subsection (k)(2) states that if the individual loses any right, or entitlement under federal law, the information must be disclosed to the individual upon request unless it would threaten the identity of a government informant.[280] Many of the DHS specific exemptions claimed under (k)(1) and (k)(2) are also encompassed in (j)(2).[281]

B. Undermining Trust in the Privacy Act: Potential Misuse and Overuse of Privacy Act's Exemptions by DHS

DHS's recent exemption claims under the September 2017 DHS Notice is consistent with the post-9/11 practice of relying upon certain facets of the Privacy Act to bypass key requirements of the Privacy Act. Since the terrorist acts of September 11, 2001, DHS has avoided the record access

277. *See* § 552a(k)(1)–(2):

> (k) Specific exemptions.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is--
>
> (1) subject to the provisions of section 552(b)(1) of this title;
>
> (2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence[.]

Id.; *see also* Appendix C.

278. § 552a(k)(1) ("subject to the provisions of section 552(b)(1) of this title[.]"); *see also* Appendix C.

279. § 552(b)(1)(A)-(B):

> (b) This section does not apply to matters that are--
>
> (1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order[.]

Id.

280. § 552a(k)(2); *see also* Appendix C.

281. *Compare* Appendix B, *with* Appendix D.

requirements of the Privacy Act in ways that could be viewed as directly oppositional to the legislative intent of the law, as it was originally considered and passed by Congress in 1974.

For example, DHS has increasingly claimed exemptions under the Privacy Act. In November 2005, the DHS Office of the Inspector General (OIG) claimed exemption under Privacy Act for its "Investigations Data Management System."[282] In October 2008, DHS claimed exemptions from the Privacy Act for Grievances, Appeals, and Disciplinary Action.[283] In December 2008, DHS claimed an exemption of non-criminal investigative information.[284] DHS also announced in December 2008 that it would maintain a record system to record individuals involved in international trade and claimed law enforcement exemptions under the system.[285] In September 2013, DHS created a record collection system for TSA's voluntary PreCheck program that pre-screens low risk passengers to expedite screening at airports and U.S. security checkpoints, and claimed multiple Privacy Act exemptions.[286]

On May 4, 2017, DHS invoked the law enforcement exemption of the Privacy Act, limiting access to the FALCON database system of records.[287]

282. Privacy Act of 1974; Implementation of Exemptions, 70 Fed. Reg. 67,931, 67,931 (Dep't of Homeland Sec. Nov. 9, 2005) (claiming exemptions for law enforcement and investigatory purposes; contending that transparency can reveal information that could threaten current investigations or the safety of confidential informants).

283. Privacy Act of 1974: Implementation of Exemptions; Grievances, Appeals, and Disciplinary Action System of Records, 73 Fed. Reg. 62,214, 62,215 (Dep't of Homeland Sec. Oct. 20, 2008) (claiming exemptions for law enforcement and national security reasons pertaining to electronic and paper records related to DHS functions).

284. Privacy Act of 1974: Implementation of Exemptions; DHS/USSS-003 Non-Criminal Investigation Information System, 73 Fed. Reg., 77,543 77,543–44 (Dec. 19, 2008) (DHS/USSS claiming exemption for the non-criminal investigative information system for investigation of individuals involved in non-criminal statutory investigations; claiming exemptions for information that may concern training, techniques, and confidential information of USSS agents).

285. Privacy Act of 1974: Implementation of Exemptions; DHS/CBP—010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities, 73 Fed. Reg. 77,541, 77,541–42 (Dec. 19, 2008) (updating system of records of individuals engaged in international trade in CBP regulated/licensed activities; claiming exemptions for law enforcement and national security reasons and to prevent individuals under investigation from frustrating the investigatory process).

286. Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security Transportation Security Administration, DHS/TSA–021, TSA Pre✓™ Application Program System of Records, 78 Fed. Reg. 55,657, 55,657 (Sept. 11, 2013) ("TSA is establishing this new system of records . . . to perform a security threat assessment to identify individuals who present a low risk to transportation security."). DHS claims exemptions apply to the new system of records: "For these records or information only, as necessary and appropriate to protect such information, in accordance with 5 U.S.C. 552a(k)(1) and (k)(2), DHS also will claim the original exemptions for these records or information from the following Privacy Act (5 U.S.C. 552a) subsections: (c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f)." *Id.* at 55,658.

287. Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Immigration and Customs Enforcement-016 FALCON Search and Analysis System of Records, 82 Fed. Reg. 20,844, 20,844–46 (May 4, 2017).

As discussed above, the FALCON Search and Analysis System of Records is an ICE data tool used by the Office of Homeland Security Investigations. Social media surveillance appears to be enhanced through enabling ICE to conduct research and analysis of multiple databases through FALCON.[288]

In June and July 2017, the Trump Administration further published several Federal Register Notices pursuant the Privacy Act, purportedly to prevent individuals who otherwise might be able to access records under the Privacy Act from accessing information from DHS systems of record. For instance, on June 14, 2017, DHS published a Federal Register Notice claiming the law enforcement exemption for the protection of property of the DHS system of records.[289] On July 17, 2017, DHS claimed the law enforcement exemption of the "Notice of Arrival and Departure System of Records."[290] On July 27, 2017, DHS published a Federal Register Notice claiming the law enforcement exemption of all "Foreign Access Management System of Records."[291]

The use of the Privacy Act to limit access to information to immigrants and noncitizens appears to be a priority for the Trump Administration. On January 25, 2017, shortly after Trump's inauguration, Privacy Act protections were eliminated for individuals who were not U.S. citizens or Lawful Permanent Residents.[292] An Executive Order titled, "Enhancing Public Safety in the Interior of the United States," directs federal agencies to "ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information" in a manner consistent with law.[293]

---

288. *Id.*

289. Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records, 82 Fed. Reg. 27,218 (June 14, 2017) (DHS claiming law enforcement exemption is necessary to protect activities of DHS and prevent individuals subject of the information from frustrating DHS operations).

290. Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/United States Coast Guard-029 Notice of Arrival and Departure System of Records, 82 Fed. Reg. 32,613, 32,613 (July 17, 2017) (DHS claiming exemptions will help DHS/USCG to help ensure maritime safety and security because information in records "may be used to support DHS national security or law enforcement activities.").

291. Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/ALL -039 Foreign Access Management System of Records, 82 Fed. Reg. 34,884 (July 27, 2017) (DHS claiming exemptions for these records because they relate to national security, law enforcement, intelligence activities, and immigration).

292. Exec. Order No. 13,768, 82 Fed. Reg. 8,799 (Jan. 30, 2017), https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/ [https://perma.cc/NE8 U-D9H3].

293. *Id.* ("Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."); *see*

The use of the law enforcement exemption in the case of the September 2017 DHS Notice further raises concerns beyond restricting access to information. Experts observe that DHS claims to the broad exemptions under the Privacy Act will prevent individuals from understanding how DHS or the federal government may use the social media data in adverse actions. Specifically, DHS claims multiple Privacy Act exemptions in the September 2017 DHS Notice, including the Privacy Act's law enforcement exemption, in order to justify the withholding of "agency procedures whereby individuals can be notified that the system contains their [social media and other] records, and procedures for accessing or contesting the content of records, as would otherwise be required by the Privacy Act [if the exemption had not been claimed]."[294]

As a result of the broad claim of exemptions under the Privacy Act by DHS, and due to the fact that the social media data may be used to inform multiple intelligence products that are part of complex law enforcement and national security data analytic environments, the accuracy of the algorithms or data analysis conducted by DHS or other federal agencies cannot be assessed and checked for inaccuracies by the individual.[295] At least one commenter observed that the law enforcement exemption did not appear to be "consistent with the Department's own description of its functions and purposes[,]" which "are primarily civil rather than criminal."[296] In response to the September 2017 DHS Notice, the commenter asserted: "Certainly, the trust and confidence of the public is a worthwhile goal for any governmental system of records, but especially one with such far-reaching impact on the lives of so many categories of stakeholders."[297]

The legislative history reveals that Congress intended the Privacy Act's exemptions should be kept to an "absolute minimum."[298] Exemptions

also DHS Memorandum by Jonathan Cantor, DHS Acting Chief Privacy Officer, *Privacy Policy Guidance Memorandum* (Apr. 17, 2017) (implementing Executive Order 13,768, "Enhancing Public Safety in the Interior of the United States on January 25, 2017"); Gabby Orr & Andrew Restuccia, *How Stephen Miller Made Immigration Personal*, POLITICO (Apr. 22, 2019, 5:01 AM), https://www.politico.com/story/2019/04/22/stephen-miller-immigration-trump-1284287 [https://perma.cc/TQ3B-WNN6] (describing how eliminating Privacy Act protections for non-citizens potentially facilitated ability of DHS to publicize the "full names and pending criminal charges—in press releases about immigrants [DHS] had apprehended, detained, or planned to deport[]").

294. *Id.*

295. SOCIAL MEDIA MONITORING REPORT, *supra* note 1, at 6–7 (explaining "the reliability of the information ingested by these systems is not verified; DHS has exempted them from the relevant requirements of the Privacy Act, and there are functionally no mechanisms for the individuals whose information is included to challenge the accuracy of the data.").

296. *Id.* at 5 (contending that the DHS Notice published on September 18, 2017, titled, "Privacy Act of 1974; System of Records," included a predominantly civil law purpose in updating the DHS system of records).

297. NEILSON, *supra* note 62, at 5 n.8.

298. S. REP. NO. 93-1183, *supra* note 31, at 20.

should only be allowed for national defense, foreign policy, and certain law enforcement and intelligence matters where "access and challenge rights are found to damage the purpose for which the information was collected."[299] Allowing exemptions only in these scenarios encourages government accountability, efficient government operations, and a "public sense of social justice."[300] Congress explained that "'authentic rights to access and challenge'" to the government's policies under the Privacy Act will force government to develop persuasive and legitimate reasons to support those policies.[301]

Congress further underscored the need to avoid secrecy. The legislative history explained that: "The [U.S. Senate] Committee [on Government Operations] believes that it is fundamental to the implementation of any privacy legislation that no system of personal information be operated or maintained in secret by a Federal agency."[302] The Committee noted that the government should refrain "from compulsory data collection" systems to respect the freedom and privacy interests of the citizenry.[303] In addition, the Committee recognized the need not "to jeopardize the collection of intelligence information related to national defense or foreign policy, or . . . . [expose classified information to] persons who do not have an appropriate security clearance or need to know."[304] At the same time, Congress also made clear that the Privacy Act exemptions relating to national security and classified information was "not intended to provide a blanket exemption to all information systems or files maintained by an agency which deal with national defense and foreign policy information."[305]

From the Privacy Act's legislative record, it can be discerned that it was Congress's intent that the exemptions for intelligence information and information related to law enforcement investigations should be limited to "certain areas of federal records [that] are of such a highly sensitive nature that they must be exempted from its provisions. . . .[for example,] a general exemption from most of the bill's operative provisions to systems of records maintained by the Central Intelligence Agency and those used for criminal

299. *Id.* at 21.

300. *Id.*

301. *Id.* at 21 (quoting Report submitted to the U.S. Dep't of Justice by Project SEARCH, Committee on Security and Privacy, Technical Report No. 2 at 28 (July 1970)).

302. *Id.* at 74.

303. *Id.* at 45 (explaining intent of Subsection 201(a) of the Privacy Act: "'[I]n terms of privacy[,] there should be a general policy to extend the zones of personal and group freedom from compulsory data collection so that matters that ought not to be considered in making decisions about individuals do not become part of the formal record at all'") (quoting National Academy of Science recommendation).

304. *Id.* at 74.

305. *Id*.

justice purposes[.]"[306] Even for agencies that fall under the exemptions, the federal agencies must publish in the Federal Register "certain identifying characteristics about virtually all systems of records under their control . . . [t]he objective of the bill is that there be no 'secret' government system of records containing personal information about individuals."[307]

Congress observed that in order to protect civil liberties, "[n]ever should economy or efficiency or administrative convenience be used to justify the exemption from or modification of any of the safeguard requirements set forth in this bill."[308] Exemptions should only apply when societal interests overwhelmingly outweigh individual privacy.[309] The limited exemptions in place were intended to protect against the release of information that had the potential to threaten national security interests or the potential to interfere with an ongoing criminal investigations, for example. Congress explained that the exemptions were intended to be read very narrowly by the federal agencies and "when exemptions must be made, they must be defined in very specific terms."[310] "By narrowing the exemption categories and defining them in specific terms related to the use of records rather than to the agency maintaining them," Congress hoped to assure the public "that the constitutional rights of individuals w[ould] be protected and w[ould] not be sacrificed to administrative discretion, expediency or whim."[311]

CONCLUSION

The relationship between citizen and state is rapidly changing in profound ways in the digital age.[312] This is a direct consequence of a rapidly evolving digital economy that privacy experts such as Shoshana Zuboff describe as a surveillance economy and surveillance capitalism and what Julie Cohen has referred to as informational capitalism and the surveillance-

306. *Privacy Act of 1974*, H. REP. NO. 93-1416, REPORT OF THE U.S. HOUSE COMMITTEE ON GOVERNMENT OPERATIONS TO ACCOMPANY TOGETHER WITH ADDITIONAL VIEWS [TO ACCOMPANY H.R. 16373] 3 (1974) [hereinafter H. REP. NO. 93-1416] (elaborating that the general exemption from the Privacy Act encompassed criminal justice databases "such as computerized systems of the National Crime Information Center (NCIC), maintained by the Federal Bureau of Investigation, and other Federal criminal history file systems.").

307. *Id.* at 4.

308. *Id.* at 37.

309. *Id.*

310. *Id.*

311. *Id.* at 38.

312. *See generally* COHEN, *supra* note 4; CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE (Jeffrey Rosen & Benjamin Wittes eds., 2011); DONOHUE , *supra* note 10; GRANICK, *supra* note 8; GRAY, *supra* note 4; JON L. MILLS, PRIVACY: THE LOST RIGHT (2008); Nissenbaum, *supra* note 4; JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE (2004); SLOBOGIN, *supra* note 4; BENJAMIN WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE: ROBOTS AND GERMS, HACKERS AND DRONES (2015).

innovation complex.[313] The digital age and the Information Society is also leading to what constitutional law scholars Jack Balkin and Sanford Levinson refer to as "The National Surveillance State."[314]

The introduction of social media data collection programs by DHS requires congressional approval or some other legal support, as the Privacy Act does not give DHS or any other federal agency the authority to collect data. A Federal Register Notice announcing a modification of a system of records under the Privacy Act does not provide sufficient legal justification for the vast expansion of a system of records to include social media platforms. To the extent that it could be argued that the social media data collection by DHS might create a new system of records, it is inappropriate to characterize social media data collection within the A-File system as simply updating an existing system of records. Characterizing social media data collection as a modification of an existing system of records routinizes social media data collection without congressional approval. This represents a new phase of bureaucratized surveillance. Careful attention must be paid to understand how DHS and other federal agencies increasingly collect and analyze social media data in programs and methods not expressly identified as surveillance or intelligence gathering programs.

New intelligence products which aggregate social media data and facilitate automation of database screening and algorithmic decisionmaking move beyond a mere update to an existing system of records that mandates disclosure under the Privacy Act. Rather, the addition of social media data into surveillance programs may constitute the establishment of an entirely new system of records for which congressional approval is required. When an agency wishes to revise or establish a system of records, the agency must go farther than notifying the public that modifications have been made—the agency should explain why the system of records was revised or established, explain the purposes and routine uses of the new types of data being collected in detail, and explain how it will impact the categories of individuals being recorded. The congressional purpose and intent of the Privacy Act is subverted when agencies make vast "updates" and "modifications" to its systems of records, and use exemptions to bypass the Privacy Act's requirements that individuals would have access to the data being collected on them.

The social media data collection programs recently introduced by DHS

313. ZUBOFF, *supra* note 1, at 94; COHEN, *supra* note 4; Julie E. Cohen, *The Surveillance-Innovation Complex: The Irony of the Participatory Turn*, *in* THE PARTICIPATORY CONDITION IN THE DIGITAL AGE 207–26 (Darin Barney et al. eds., 2016).

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

and other federal agencies provide an important window into understanding this new form of records system maintenance. The collection will encompass social media data on both citizens and noncitizens, and was not explicitly authorized by Congress.[315] Further, widespread social media surveillance practices across multiple agencies have been underway for nearly a decade.[316] Social media surveillance programs by federal agencies are largely unregulated and the announcement of social media data collection programs pursuant to the reporting requirements of the Privacy Act deserves careful legal attention. The distinction between social media intelligence, on the one hand, and social media collection for records system retention is blurring. The privacy impact of systemized and routinized social media data collection will continue to be obscured without more fully appreciating how federal agencies such as DHS may be accomplishing intelligence goals through the Privacy Act in a way that is directly opposite of what Congress intended to accomplish by enacting the Privacy Act.

In enacting the Privacy Act of 1974, Congress intended to restore public confidence in government data collection and recordkeeping. Congress warned that, "[a]ccelerated data sharing of such personally identifiable information among increasing numbers of Federal agencies through sophisticated automated systems," could lead to data misuse and abuse.[317] Congress observed that the technological advances in databases and digitization of records, "coupled with the recent disclosures of serious abuses of governmental authority represented by the collection of personal dossiers, illegal wiretapping, surveillance of innocent citizens, misuse of income tax data, and similar types of abuses, have helped to create a growing distrust, or even fear of their Government in the minds of millions of Americans."[318]

Passage of the Privacy Act was meant to engender trust. Trust in the Privacy Act is at risk when the Act's notice requirements announce the social media data collection and analysis systems under the guise of modifying record collection and retention protocols. This Article concludes that the social media data collection proposed by DHS requires express legislative authorization.

315. SOCIAL MEDIA MONITORING REPORT, *supra* note 1, at 5. Important research has been published on government secrecy and the need for transparency in agency action, including intelligence agencies. *See, e.g.*, ELIZABETH GOITEIN, THE NEW ERA OF SECRET LAW 44–47 (2016); Louis J. Virelli III & Ellen S. Podgor, *Secret Policies*, 2019 ILL. L. REV. 463 (2019); David Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257 (2010); Adam M. Samaha, *Government Secrets, Constitutional Law, and Platforms for Judicial Intervention*, 53 UCLA L. REV. 909 (2006).

316. *See generally* SOCIAL MEDIA MONITORING REPORT, *supra* note 1, app. at 35–36.

317. H. REP. NO. 93-1416, *supra* note 306, at 3.

318. *Id.*

APPENDIX A

General Exemptions of the Privacy Act of 1974

Privacy Act 5 U.S.C. § 552a(j)(1) **General Exemptions: CIA**
The Privacy Act's "General Exemptions" are divided into two parts: 5 U.S.C. § 552a(j)(1) and 5 U.S.C. § 552a(j)(2). The "General Exemptions" under 5 U.S.C. § 552a(j)(1) applies to a system of records maintained by the CIA: (j) General exemptions.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is (1) maintained by the Central Intelligence Agency[.]
Privacy Act 5 U.S.C. § 552a(j)(2) **General Exemptions: Law Enforcement**
The Law Enforcement "General Exemptions" under the Privacy Act provides that an agency may claim that certain provisions of the Privacy Act are exempted when a system of records is: maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of

> the criminal laws from arrest or indictment through release from supervision.
>
> At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

APPENDIX B

Privacy Act's General Law Enforcement Exemptions Claimed by DHS Under 5 U.S.C. § 552a(j)(2) in 82 Federal Register 43,556: "DHS Notice of Modified Privacy Act System of Records" (September 18, 2017)

5 U.S.C. § 552a	**General Exemptions: Privacy Act Provision DHS Claims is Exempted Under 5 U.S.C. § 552a(j)(2) (General Exemptions: Law Enforcement)**
(c)(3)	5 U.S.C. § 552a(c)(3): [E]xcept for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request[.]
(c)(4)	5 U.S.C. § 552a(c)(4): [I]nform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.
(d)	5 U.S.C. § 552a(d): Access to records.—Each agency that maintains a system of records shall—(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence; (2) permit the individual to request amendment of a record pertaining to him and— (A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and (B) promptly, either— (i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or (ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of

	the agency or an officer designated by the head of the agency, and the name and business address of that official; (3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section; (4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and (5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.
(e)(1)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President[.]
(e)(2)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs[.]

(e)(3)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(3) [I]nform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual— (A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on him, if any, of not providing all or any part of the requested information[.]
(e)(4)(G)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include— (e)(4)(G)("the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him[.]
(e)(4)(H)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include— (e)(4)(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content") ("the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content[.]

(e)(4)(I)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include— (e)(4)(I) the categories of sources of records in the system[.]
(e)(5)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination[.]
(e)(8)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record[.]
(e)(12)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(12) if such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.
(f)	5 U.S.C. § 552a(f) Agency rules.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall— (1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him; (2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual; (3) establish procedures for the disclosure to an

	individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him; (4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and (5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record. The Office of the Federal Register shall biennially compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.
(g)(1)	5 U.S.C. § 552a(g)(1) Civil remedies.—Whenever any agency (A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection; (B) refuses to comply with an individual request under subsection (d)(1) of this section; (C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or (D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall

	have jurisdiction in the matters under the provisions of this subsection.
(h)	5 U.S.C. § 552a(h) For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

APPENDIX C

Specific Exemptions of the Privacy Act of 1974

Privacy Act 5 U.S.C. § 552a(k)(1) **Specific Exemptions: Classified Information for National Defense or Foreign Policy**
The Privacy Act's "Specific Exemptions" are divided into two parts: 5 U.S.C. § 552a(k)(1) and 5 U.S.C. § 552a(k)(2). Under 5 U.S.C. § 552a(k)(1), the Privacy Act states that the (k)(1) specific exemptions are: 5 U.S.C. § 552a(k): The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is— (1) subject to the provisions of section 552(b)(1) of this title[.] 5 U.S.C. § 552(b)(1) provides that: This section does not apply to matters that are— (1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order[.]
Privacy Act 5 U.S.C. § 552a(k)(2) **Specific Exemptions: Head of Agency Promulgated Rules to Cover Other Investigatory Material**
The Privacy Act's "Specific Exemptions" under the Privacy Act provides that an agency may claim that certain provisions of the Privacy Act are exempted when a system of records is: 5 U.S.C. § 552a(k): The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is— . . . (2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided,

> however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence[.]

APPENDIX D

Privacy Act's Specific Exemptions Claimed by DHS in 82 Federal Register 43,556: "DHS Notice of Modified Privacy Act System of Records" (September 18, 2017)

5 U.S.C. § 552a	**Specific Exemptions: Privacy Act Provision DHS Claims is Exempted Under 5 U.S.C. § 552a(k)(1) (Specific Exemptions Relating to Classified Information) and 5 U.S.C. § 552a(k)(2) (Specific Exemptions Promulgated by Head of Federal Agency to Cover Other Investigatory Material)**
(c)(3)	5 U.S.C. § 552a(c)(3): [E]xcept for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request[.]
(d)	5 U.S.C. § 552a(d): Access to records.—Each agency that maintains a system of records shall—(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence; (2) permit the individual to request amendment of a record pertaining to him and— (A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and (B) promptly, either— (i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or (ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

	(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section; (4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and (5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.
(e)(1)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President[.]
(e)(4)(G)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include— (e)(4)(G)("the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him[.]

(e)(4)(H)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include— (e)(4)(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content") ("the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content[.]
(e)(4)(I)	5 U.S.C. § 552a(e) Each agency that maintains a system of records shall— (e)(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include— (e)(4)(I) the categories of sources of records in the system[.]
(f)	5 U.S.C. § 552a(f) Agency rules.--In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall— (1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him; (2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual; (3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him; (4) establish procedures for reviewing a request from an individual concerning the amendment of any record or

	information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and (5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record. The Office of the Federal Register shall biennially compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.