Dear ILW Participants: This piece, forthcoming in the Washington University Law Review, is a work-in-progress. Please do not cite or circulate. Thank you. Margaret

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, 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 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 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 required notice announces the expansion of new social media data collection and analysis systems under the guise of modifying record collection and

† Margaret Hu, Kenan Visiting Professor, Kenan Institute for Ethics, Duke University (Spring-Fall 2019); Associate Professor of Law, Washington and Lee University School of Law. This work benefitted from the thoughtful feedback received from John Bagby, 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.
This Article concludes that the social media data collection proposed by DHS requires express legislative authorization.
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 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.” 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 . . .”

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).

The disclosures of former National Security Agency (NSA)


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.
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 programs revealed by the Snowden disclosures, 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 and constitutional consequences of the Snowden revelations and ubiquitous surveillance have focused on activities that are explicitly recognized as foreign intelligence gathering and national security surveillance activities.11 This Article,

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 9; 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 AGE (2016); GRANICK, supra note 9; GREENWALD, supra note 9; Mills in AFTER SNOWDEN, supra note 9; Hu, Taxonomy, supra note 9; 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, THE FUTURE OF FOREIGN INTELLIGENCE, supra note 10; William C. Banks, Programmatic Surveillance and FISA: Of Needles in Haystacks, 88 TEX. L. REV. 1633 (2010); Laura K. Donohue,
however, does not focus on foreign intelligence gathering, national security surveillance, or law enforcement data collection that is self-described by the federal government as surveillance.

At the outset, it is critical to admit that social media surveillance or open source intelligence gathering that relies on publicly available data is complicated significantly by the Fourth Amendment’s third-party doctrine. Under a straightforward reading of the third-party doctrine, information shared through a social media platform would not be considered private. Therefore, social media data collection would not appear to fall within the protection of the Fourth Amendment’s reasonable expectation of privacy test under the third-party doctrine.

Future scholarship will address how the recent Supreme Court decision in Carpenter v. United States, forces a reexamination of the reach and scope of the Fourth Amendment in light of digital surveillance tools, including social media surveillance.

This Article, however, does not analyze the constitutional impact of social media data collection by DHS or other federal agencies. 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. Under the public notice requirements of the


13 Id.
Privacy Act of 1974, DHS notified the public that record systems would be modified to encompass social media data collection. These programs should be understood as representing a bureaucratized evolution of digital surveillance or cybersurveillance. 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 imposed on the intelligence community by foreign intelligence surveillance law or the protections of the Fourth Amendment of the U.S. Constitution. 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, illustrates this phenomena.

---


17 See infra note 22, and 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), https://www.lawfareblog.com/new-authorities-military-cyber-operations-and-surveillance-including-tma (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).


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

\(^{21}\) 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 . . . .”).
Register by DHS on September 18, 2017. The Notice modifies a specific system of records: “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.”


Id. Alien Files (A-File records) are defined as:

[A] system of records containing 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.

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 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
registration numbers and related A-Files are created for immigrants and certain categories of non-immigrants who are granted employment authorization. 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. DHS retains these records after these individuals gain the status of naturalized U.S. citizens.

The September 18, 2017, DHS “Notice of Modified Privacy Act System of Records,” for instance, revealed that social media data can now be retained 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 43 million foreign-born individuals currently residing in the United States.

DHS claims that the September 18, 2017, Notice conforms with the existing protocol. DHS, in a response to media requests to clarify the Notice, stated: “The notice did not announce a new policy. The notice simply reiterated existing DHS policy regarding the use of social media.” Yet, the Notices issued by DHS indicate that social media screening is emerging as a routinized aspect of DHS vetting procedures. The Notices also signal 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 surveillance promulgated under federal agency action is inconsistent with the law. Part II provides a summary of how DHS has engaged in social media surveillance since at least 2010. It also attempts to contextualize DHS social media surveillance practices within other algorithmic decisionmaking systems that are increasingly dependent upon data gathering, including the gathering of social media data. Part III focuses on Extreme Vetting as a case study to 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 the expansion of new 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.31 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. Consequently, social media data collection programs proposed by DHS or 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 can be viewed as ironic. Part I.A provides an overview of the legislative background to the Privacy Act covering the (1) history, (2) purpose, and (3) statutory requirements imposed on federal agencies. Part I.B summarizes the concerns of commenters involving the (1) constitutional impact, (2) Privacy Act and administrative law issues, and (3) apprehension regarding data collection, storage, and use stemming from the DHS System of Records Notice published pursuant to the Privacy Act.

31 Social Media Monitoring Report supra note 22, at 5.
requirements to notify the public of an “update” to the DHS/USCIS-ICE-CBP-001 Alien File, Index, and National File Tracking System of Records published in the Federal Register on September 18, 2017.\footnote{Privacy Act of 1974, 82 Fed. Reg. at 43,556.}

A. Introduction to the Privacy Act of 1974

(1) Legislative History and Amendment to the Privacy Act

In a legislative statement entered by Congress, upon passage of the Privacy Act, the intention of the Act was made clear: “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.”\footnote{120 Cong. Rec. 12,646 (May 1, 1974) (Remarks of Sen. Ervin (D-N.C.) on S. 3418).} The legislative history includes this prescient statement: “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.”\footnote{Id. at 12,647.}

In a Hearing Before the Subcommittee on Constitutional Rights: Federal Data Banks, Computers, and the Bill of Rights, Part I, 92nd Congress, 1971, 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 privaey,” to help the citizenry embrace the notion that a democratic society requires “freedom from unwarranted intrusion.”\footnote{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).} The Act also recognized the need to “put specific limits on those who would gather and use this information.”\footnote{Id. at 304.}

In a committee report submitted by the U.S. Senate Committee on Government Operations, intended to accompany the Privacy Act,
S.3418, titled Protecting Individual Privacy in Federal Gathering, Use and Disclosure of Information, Congress explained that 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 constitutional rules in the computerization, collection, management, use, and disclosure of personal information about individuals.” The Act further aimed to “promote accountability, responsibility . . . [and prevent] illegal, unwise, overbroad, investigation and record surveillance of law-abiding citizens[.]” 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.

In 1988, the Privacy Act was amended to incorporate the Computer Matching and Privacy Protection Act (CMPPA). 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. 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. The CMPPA is intended to complement the privacy goals of the Privacy Act, including the integrity of data use

38 Id.
39 Id. at 2-3.
41 5 U.S.C. § 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.”).
42 Id.
disclosure of data used by the federal government through computerized matching.\textsuperscript{43}

(2) Purpose of the Privacy Act

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.\textsuperscript{44} 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.”\textsuperscript{45} 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 allowed under specified statutory exceptions.\textsuperscript{46}

Passage of the Privacy Act of 1974 was precipitated 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.”\textsuperscript{47}

(3) Statutory Requirements Imposed on Federal Agencies by the Privacy Act

The Privacy Act of 1974 was designed to “provide[s] certain


\textsuperscript{44}See, \textit{e.g.}, 5 U.S.C. § 552a(a)(5) (defining “system of records”); \textit{see also supra} note 37.

\textsuperscript{45}5 U.S.C. § 552a(a)(5).

\textsuperscript{46}Id. at § 552a(b)(1-12). \textit{See also infra} note 248.

safeguards for an individual against an invasion of personal privacy” by the federal agencies. 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.

The Privacy Act also generally provides the right of access to federal agency records where the person is a subject of those records. 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 will be discussed in more detail in Part IV.B.

In contrast to exemptions, conditions of disclosure under the Privacy Act describe certain conditions present for federal agencies to legally disclose information to others—including other federal agencies, contractors, and other private individuals—that it has compiled on an individual. 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. Census Bureau and the Bureau of Labor Statistics; routinized use within a U.S. government agency; record archival purposes “as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government”; civil or criminal

---

49 5 U.S.C. §§ 552a(g)(1)(D), (g)(4)(A).
50 Id. at § 552a.
51 See 5 U.S.C. § 552a(b)(1-12). See also infra note 248.
52 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.”).
53 5 U.S.C. § 552a(b)(4-5).
54 Id. at § 552a(b)(3).
55 Id. at § 552a(b)(6).
law enforcement purposes;\textsuperscript{56} congressional investigations;\textsuperscript{57} and to achieve other administrative objectives.\textsuperscript{58}

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.\textsuperscript{59} 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.\textsuperscript{60}

Under the requirements of the Privacy Act, when a federal agency revises its system of records, the agency must publish a notice in the Federal Register that describes the revision.\textsuperscript{61} For instance, the notice in the 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.”\textsuperscript{62} The Privacy Act provides that at least a 30-day notice must be provided in the Federal Register of “any new use or intended use of the information in the system, and provide any opportunity for interested persons to submit written data, views, or arguments to the agency.”\textsuperscript{63} The Notice in the Federal Register regarding the “Modified Privacy Act System of Records”\textsuperscript{64} by DHS to include the collection of social media data, therefore, fell within these mandatory reporting requirements that dictated the publication of the change in collection and use of system records.

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

The DHS “Notice of Modified Privacy Act System of Records” published on September 18, 2017, was highly controversial and

\textsuperscript{56} Id. at § 552a(b)(7).
\textsuperscript{57} Id. at § 552a(b)(9).
\textsuperscript{58} Id. at § 552a(b)(1).
\textsuperscript{59} Id. at § 552a(e)(3)(A).
\textsuperscript{60} Id. at § 552a(a)(4).
\textsuperscript{61} Id. at § 552a(e)(4).
\textsuperscript{62} Id. at § 552a(e)(4)(D).
\textsuperscript{63} Id. at § 552a(e)(11).
\textsuperscript{64} 82 Fed. Reg. 43,556 (“ACTION: Notice of Modified Privacy Act System of Records.”).
resulted in over 2,900 comments submitted to DHS by the public.\textsuperscript{65} 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,\textsuperscript{66} DHS published the Notice to describe the collection and use of social media data.\textsuperscript{67} 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.\textsuperscript{68} DHS also indicated that other uses of the social media data would include investigatory purposes including criminal law enforcement and counterterrorism goals.\textsuperscript{69}

1. Constitutional Law Concerns

The use of the Privacy Act’s mandate to give public notice of a revision of system records\textsuperscript{70} to facilitate social media surveillance has raised 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 comments responding to the DHS “Notice of Modified Privacy Act System of Records” published on September 18, 2017, raised concerns that were intersectional in nature. Several commenters noted that social media surveillance combined constitutional concerns with


\textsuperscript{66} 5 U.S.C. § 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[.]”).

\textsuperscript{67} Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,556 (Sept. 18, 2017).

\textsuperscript{68} Id. at 43,556-57.

\textsuperscript{69} Id. at 43,557-63.

\textsuperscript{70} 5 U.S.C. § 552a(e)(4).
technological capacity issues, such as whether the data collected could accurately serve the objectives articulated by DHS.\textsuperscript{71}

Comments generated by the public and submitted to DHS in response to the Federal Register notices include the following concerns under the First Amendment: Chilling of speech and expressive freedoms and infringing upon association rights.\textsuperscript{72} Other First Amendment concerns included whether requests for social media handles and aliases could potentially jeopardize anonymous speech, and whether analysis of social media could result in political and religious targeting.\textsuperscript{73}

A coalition letter that included 27 organizations—such as the ACLU, Brennan Center for Justice, Center for Democracy & Technology, the Electronic Frontier Foundation, and Human Rights Watch—and other expert responses, expressed concerns regarding the warrantless seizure of data and mass cyber searches of social media information in violation of the Fourth Amendment.\textsuperscript{74} A comment letter sent to DHS by the Electronic Privacy Information Center further shared the coalition’s concern regarding the infringement of First Amendment freedoms, and also expressed concern about the accuracy and integrity of the social media data collected.\textsuperscript{75} Some commenters also noted that the meaning of messages conveyed over social media might be difficult to interpret.

\textsuperscript{71} See, e.g., Coalition Letter Opposing DHS Social Media Retention, CENTER FOR DEMOCRACY AND TECHNOLOGY (Oct. 19, 2017) [hereinafter “Coalition Letter”], https://cdt.org/insight/coalition-letter-opposing-dhs-social-media-retention/ [https://perma.cc/LK7C-22VJ]; Scott, supra note 53, at 16.\textsuperscript{72} Id.\textsuperscript{73} Coalition Letter, supra note 50.\textsuperscript{74} 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/; EFF, DHS Should Stop Social Media Surveillance, supra note 60; Coalition Letter, supra note 50; Scott, supra note 53, at 19; Sellars, supra note 139; Patel & Panduranga, supra note 194.\textsuperscript{75} Comment submitted by Jeramie Scott and the Electronic Privacy Information Center (EPIC) (Oct. 18, 2017), https://epic.org/apa/comments/EPIC-DHS-Social-Media-Info-Collection.pdf. See also Social Media Monitoring Report supra note 22, at 5.
and discern. Multiple comments expressed concern that naturalized U.S. citizens would be relegated to “second-class citizenship”, as under the Notice the social media data could be collected on both foreigners and naturalized U.S. citizens.

2. Privacy Act and Administrative Law Concerns

Multiple commenters noted that the DHS Notice appeared 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, observed 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. The New York City Bar further noted 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. Other comments expressed concern about the administrative procedure followed, and whether the Privacy Act was being honored in spirit, even though it may have been honored under the letter of the law.

3. Data Collection, Storage, and Use Concerns

Civil rights and other organizations raised concerns about the vagueness of the Notice. The Notice, for instance, failed to define “social media” or “search results.” 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. The coalition noted that the failure to explain exactly how the social media data would be used, currently and into the future, with any specificity, raised concerns regarding how such data might invite

76 See, e.g., Coalition Letter, supra note x; comment submitted by Jeramie Scott and EPIC, supra note 75. See also Social Media Monitoring Report supra note 22 at 4-5.
77 See, e.g., Coalition Letter, supra note X; Neilson, supra note X.
78 Neilson, supra note X, at 4.
79 Id. at 2-5.
80 Neilson, supra note x, at 3.
81 Coalition Letter, supra note X.
82 Id.

Multiple comments reflected deep reservation about the new social media collection activities by the federal government in light of unanswered questions. These questions included: 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;\footnote{Id. at 6.} how the storage of the data in the A-files for up to 100 years could impact future use in automated decision making and algorithmic risk assessment;\footnote{Id.} whether such social media surveillance might increase the risk of data misuse and abuse without evidence of the benefits to national security.\footnote{Duarte, supra note x.} Some experts have suggested adding the ability to correct, access, and even destroy data collected in order to prevent power imbalances and ensure fairness and accuracy for important data driven decisions.\footnote{Neilson, supra note x, at 4; Coalition Letter, supra note 50.} Finally, several comments expressed reservation that the new social media collection protocols would effectively relegate naturalized U.S. citizens to second class citizenship status\footnote{Coalition Letter, supra note 50.} and pointed out that questions remained regarding whether social media surveillance would continue and for how long after an individual might become a naturalized U.S. citizen.\footnote{Coalition Letter, supra note 50.}

\section{II. Brief History of Social Media Intelligence}

\footnote{Id. at 6.}
To better understand how DHS uses social media data to serve intelligence objectives, 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.

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 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.\(^\text{90}\) 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 . . . \(\text{91}\) 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.”\(^\text{92}\) At the same, Citron predicted that the federal government’s use of social media would introduce a host of unprecedented privacy concerns.\(^\text{93}\) With a broader engagement of social media data, the federal government would


\(^{91}\) Id.

\(^{92}\) See Citron, Government 2.0, supra note 1, at 825 (internal citations omitted).

\(^{93}\) Id. at 826.
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.”

Citron’s warning proved prescient. On a pilot program basis, DHS officially commenced its experimentation with social media surveillance as early as 2010. 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.” DHS was particularly interested in harnessing social media monitoring to enhance its “situational awareness capacities.” Situational awareness 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.”

---

94 Id.
98 Id.
Also in 2010, the Electronic Frontier Foundation (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.\textsuperscript{100} 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 the Electronic Privacy Information Center (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.”\textsuperscript{101} 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 Defense Advanced Research Projects Agency (DARPA) announced an initiative titled: “Forecasting Dynamic Group Behavior in Social Media.”\textsuperscript{102} 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.”\textsuperscript{103} In order to “forecast[] dynamic group behavior in social media[,]” DARPA explained that it


\textsuperscript{103} \textit{Id.}
envisioned tools that had the capacity to scan over 1 million people, over 1,000 groups, and over 100,000 postings per day.  

Also in 2012, the FBI released a Request for Information soliciting a tool that would assist the agency in using social media surveillance and Internet surveillance through web scraping and the scraping of publicly available 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. 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.

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.” DHS provided the following legal authorities for the Directive:


B. Title 5, United States Code (U.S.C.), Section 552a, “Records Maintained on Individuals” [The Privacy Act of 1974, as amended][;]

---

104 Id.
106 Id.
C. Title 6 U.S.C. Section 142, “Privacy officer”[;]
E. Delegation 13001, “Delegation to the Chief Privacy Officer”[.]

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.”

In a six-month period in 2012, over 9,300 “item-of-interest” reports were generated by the DHS social media monitoring program.

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.* 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. The report explained that DHS utilized a

108 Id. at 1–2.
109 Id. at 2.
111 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) [hereinafter DHS’ PILOTS FOR SOCIAL MEDIA SCREENING], https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf [https://perma.cc/QTA8-H5AF].
112 Id. at 2.
“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.”\textsuperscript{113} By April 2016, DHS began testing an additional social media screening tool that was developed by the U.S. Department of Defense, Defense Advanced Research Projects Agency (DARPA) in order to screen nonimmigrant visa holders.\textsuperscript{114}

On June 23, 2016, Customs and Border Protection (CBP) of 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.”\textsuperscript{115} 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.\textsuperscript{116} 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.”\textsuperscript{117}

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.”\textsuperscript{118} Without further evidence and testing information, the report concluded that the tests “provide limited information for planning and implementing an

\textsuperscript{113} Id. at 2, n.6.
\textsuperscript{114} Id. at 2-3.
\textsuperscript{116} Id.
\textsuperscript{117} DHS’ PILOTS FOR SOCIAL MEDIA SCREENING, supra note 76, at 3-4.
\textsuperscript{118} Id. at 1.
effective, department-wide future social media screening program.”

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

The Intelligence Community (IC) is comprised of 16 IC components that are coordinated under the umbrella of the White House Office of the Director of National Intelligence (ODNI). The IC includes the National Security Agency (NSA), Central Intelligence Agency (CIA), and FBI. 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 tasked with the collection and analysis of “threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners.” 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 screening, 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.”

As DHS Directive 110-01 allows each component to establish

---

119 Id.
121 Id.
123 See, e.g., Coalition Letter, supra note X; Scott, supra note X (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”).
124 Id.
its own policies and programs regarding the operational use of social media, it is instructive to examine how one component, DHS’s U.S. Customs and Border Protection (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).125 The CIRS will deploy algorithmic decision-making and predictive tools, including the “Analytical Framework for Intelligence (AFI)” and “Intelligence Reporting System (IRS).”126 The systems will appear to 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.”127 The report will also heavily focus on analysis of associational data.128 The Notice explains that the analysis will rely upon biographic, biometric, criminal and investigatory records, and other government documents.129 By specifying that the data 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.130 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[.]”131 This suggests the system can

---

126 Id. at 44,199.
127 Id.
128 Id. at 44,198.
129 Id. at 44,200.
130 Id.
131 Id.
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.\textsuperscript{132} 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.\textsuperscript{133}

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.

\textsuperscript{132} “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[.]” \textit{id.} at 44,199.

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. 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.” 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 . . . .” Shortly before his election, Trump also announced a proposal for the “extreme vetting” of immigrants and refugees. 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.”138

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,”139 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 implementation of extreme vetting.140 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.141 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, that left the extreme vetting provisions of the first travel ban in place and appeared to expand several vetting protocols.142


---

138 Peters & Wooley, supra note 134.
140 See, e.g., Hu, Algorithmic Jim Crow, supra note XX, at 638-43; Hu, Crimmigration-Counterterrorism, supra note XX, 984-992.
141 Transcript of Testimony by John F. Kelly, DHS Secretary, Hearing Before the U.S. House of Representatives Committee on Homeland Security, Ending the Crisis: America’s Borders and the Path to Security 83 (Feb. 7, 2017), https://docs.house.gov/meetings/HM/HM00/20170207/105474/HHRG-115-HM00-Transcript-20170207.pdf. 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.
142 See, e.g., Hu, Algorithmic Jim Crow, supra note XX, at 638-43; Hu, Crimmigration-Counterterrorism, supra note XX, 984-992.
request for information from a “subset” of visa applicants included social media handles, aliases, phone numbers, and email addresses over the past five years. The notice purported to request the information as a way to “more rigorously evaluate applicants for terrorism or other national security-related visa ineligibilities[.]

As an emergency action, the notice observed that it would only be in effect for 180 days. On May 18, 2017, a coalition of 35 civil and human rights organizations—including the Brennan Center for Justice, Center for Democracy and Technology, Electronic Frontier Foundation, 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 concerns. Less than three months later, the State Department issued an additional notice proposing to make the revised collection protocol permanent.

Exactly how DHS intended to use an automated tool for social media vetting gained clarity with media revelations surrounding a DHS-hosted “Industry Day” to discuss a request for information of an industry contract to build technologies for extreme vetting. During this event, DHS circulated a document entitled: “Extreme Vetting Initiative.” This document explained that DHS intended to award contracts to the firms to assist the federal government in

---

144 Id.
145 Id.
146 Id.
149 Id.
counterterrorism-related data analysis. \textsuperscript{150} 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.\textsuperscript{151}

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.”\textsuperscript{152}

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.”\textsuperscript{153}

According to ICE, the ideal system would have the ability to “determine and evaluate an applicant’s probability of becoming a

\textsuperscript{150} Id.
\textsuperscript{151} Id.
\textsuperscript{152} Id. (quoting the ICE “Extreme Vetting Initiative” document) (DEP’T OF HOMELAND SEC., EXTREME VETTING INITIATIVE STATEMENT OF OBJECTIVES (SOO), http://www.brennancenter.org/sites/default/files/Extreme%20Vetting%20Initiate %20-%20Statement%20of%20Objectives.pdf [https://perma.cc/F2UW-GWPX]).
\textsuperscript{153} Biddle & Woodman, \textit{supra} note \textit{Error! Bookmark not defined.} (quoting the ICE “Extreme Vetting Initiative” document).
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.”

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.” DHS received a question from an anonymous contractor regarding a potential legal challenge by the American Civil Liberties Union (ACLU). 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?

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. One official stated: “The prediction is that in the near future there will be legislation addressing what you can and can’t do. . . . We will continue to do it until someone says that we can’t.”

On September 18, 2017, the DHS Privacy Office introduced a Notice under the title of “Notice of Modified Privacy Act System of Records.” DHS explained that information would be added to the

---

154 Id. (quoting the ICE “Extreme Vetting Initiative” document).
155 Id. (quoting from a Q&A session between ICE and contractors).
156 Id.
157 Id.
158 Id.
159 Id.
160 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
Alien Files (A-Files)\textsuperscript{161} 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”\textsuperscript{162} on immigrants, including permanent residents and naturalized citizens. 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.”\textsuperscript{163} This redefinition specifically includes immigrants, lawful permanent residents, and naturalized U.S. citizens’ “social media handles, aliases, associated identifiable information, and search results.”\textsuperscript{164} DHS did not define “search results.”

Those submitting comments on the new regulation noted that U.S. citizens who communicate with immigrants would be impacted by the revisions.\textsuperscript{165} Other public comments received by DHS questioned the scientific validity and efficacy of the social media screenings, noting that DHS has not offered any evidence that social media screening thwarts terroristic or criminal risks.\textsuperscript{166} Additionally,
six U.S. 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.\(^\text{167}\)

DHS, in response to media inquiries and in defense of the legality and legitimacy of the collection of social media data, explained:

This policy permits a small cadre of specifically trained [DHS United States Citizenship and Immigration Services] USCIS 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.\(^\text{168}\)

On September 24, 2017, President Trump published his third travel ban, a Presidential Proclamation titled “Enhancing Vetting


\(^{168}\) Novak, supra note 30.
Capabilities and Processes for Detecting Attempted Entry Into the United States by Terrorists or Other Public-Safety Threats.” The Proclamation emphasized the need for increased screening and vetting processes, including the collection of biometric and biographic data. The Proclamation followed DHS’s September 18, 2017, Federal Register publication of the “Notice of Modified Privacy Act System of Records,” and the CBP’s September 21, 2017, “Notice of new Privacy Act System of Records.” In October 2017, DHS issued a press release announcing new investigative procedures for refugees from eleven “high-risk” countries that included social media checks and an additional 90-day review period. The enhanced vetting procedures were issued in accordance with Section 6(a) of the second travel ban, Executive Order 13,780. These changes were implemented in January 2018.

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,” and a “Notice of Proposed Information Collection: Application for Nonimmigrant Visa.” 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 or who have visited terrorist-controlled areas are required

170 Id. at 45,170.
174 Id.
177 Id. at 13,807.
to provide the State Department with all phone number, email, and social media account history for the past five years. 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 at the federal and state level.\footnote{DHS explains that vetting uses both classified and unclassified databases for biometric and biographic screening, corroborating that vetting involves intelligence tools. For example, “refugees’ names and biographical information [are checked] against CIA population-groups-for-tougher-visa-screening-idUSKBN16U12X [https://perma.cc/6KB8-RSVV]. But see DEP’T OF HOMELAND SEC., CITIZENSHIP PROTECTION: 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].\footnote{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. at 36,181. 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].\footnote{Id. See, e.g., Sandra E. Garcia, U.S. Requiring Social Media Information from Visa Applicants, N.Y. TIMES (Jun. 2, 2019); Faiza Patel, Stop Collecting Immigrants’ Social Media, N.Y. TIMES Op-Ed (June 30, 2019), https://www.nytimes.com/2019/06/30/opinion/immigrants-social-media.html.\footnote{DEP’T HOMELAND SEC., U.S. CITIZENSHIP & IMMIGR. SERVS., REFUGEE SECURITY SCREENING FACT SHEET 6 (Aug 28, 2018) [hereinafter DHS REFUGEE SECURITY SCREENING FACT SHEET], https://www.uscis.gov/sites/default/files/USCIS/Refugee%2CAsylum%20and%20Int%27l%20Ops/Refugee-Screening_and_Vetting_Fact_Sheet.pdf [https://perma.cc/A4PR-NK5X] (“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.”).}}
and multiple other databases to automatically screen “cellphone numbers, address books, social media postings, arrest reports and intelligence assessments” 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.”

B. Extreme Vetting Initiative and Visa Lifecycle Vetting Initiative

The Extreme Vetting Initiative appears to build upon the “ICE Investigative Case Management” system (ICM). ICM allows for up to “10,000 users” to access up to “tens of millions of subject records.” Through multiple databases, both public and private, ICM “can provide ICE agents access to information on 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.” ICM is reported to be reliant upon two intelligence data systems: ICE’s FALCON and the CBP’s Analytical Framework for Intelligence (AFI). FALCON, a dataminning and

---

184 Id. (databases include those of DHS, Department of State, CIA, FBI, and National Counterterrorism Center, and Department of Defense).
185 Id.
186 DHS REFUGEE SECURITY SCREENING FACT SHEET, supra note X, at 6 (“DOD screening began in 2007 for Iraqi applicants and incrementally expanded to all refugee nationalities by 2013.”).
188 Id.
189 Id.
data analytic network, allows DHS Office of Homeland Security Investigations agents to track immigrants and conduct data analysis on cross-border crimes. ICM also grants its users access to AFI, a largely classified database. Experts have speculated that the risk assessment profiling algorithms associated with “extreme vetting” are intended to be built upon the algorithms of AFI. “‘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.”

DHS announced that the “Extreme Vetting” Initiative had been renamed the “Visa Lifecycle Vetting Initiative.” 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.” 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 the Director of

191 Id.
193 Woodman, supra note X.
194 Id. (quoting Edward Hasbrouck, Identity Project).
the Central Intelligence Agency[].\textsuperscript{197} The memo seeks “contextual information” in addition to “biographic” and “biometric” information.\textsuperscript{198}

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.”\textsuperscript{199} In other words, this DHS statement seems 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.\textsuperscript{200} 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.\textsuperscript{201} DHS pursued 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.”\textsuperscript{202}

Cutrell explained that, through the Visa Lifecycle Vetting Initiative, ICE sought continuous monitoring of social media behavior to detect “radical or extremist views.”\textsuperscript{203} ICE’s Acting Director, Thomas Homan, explained that enhanced analytical tools utilized social media data.\textsuperscript{204} Homan stated that senior analysts reviewed the leads generated from these tools before the leads were used in investigations.\textsuperscript{205}

\textsuperscript{197} Id. at 2.
\textsuperscript{198} Id. at 1.
\textsuperscript{200} Id.
\textsuperscript{201} Id.
\textsuperscript{202} Id.
\textsuperscript{203} Id.
\textsuperscript{204} Id.
\textsuperscript{205} Id.
“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.’””206 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 leads as they keep tabs on their social-media use.””207

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. The discussion in Part IV explores how the DHS System of Records Notice, titled, “Privacy Act of 1974; System of Records,” published in the Federal Register on September 18, 2017, 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. The discussion below focuses especially on the integrated data environment of the AFI system.

IV. PRIVACY AND TRUST: DISTURBANCE 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 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 DHS Notice titled, “Privacy Act of 1974; System of Records,” that was published on September 18, 2017. Without a close inspection of these provisions, it would be impossible to understand the privacy

206 Id.
207 Id.
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 exemption 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 the “systems of records” through publication in the Federal Register.208 The DHS and Department of State Notices that were issued pursuant to the Privacy Act conform to the Act’s specific agency record-keeping requirements. The DHS Notice, “Privacy Act of 1974; System of Records,” published on September 18, 2017, in the Federal Register stated in the Notice Background 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.”209 In the updating of the A-File system of records, DHS explained that it would promulgate “substantive changes” in twelve separate instances.210 Some

210 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;
“substantive changes” involved clarifying data storage and where the system is located.\textsuperscript{211} Other “substantive changes” raise potential constitutional and legal issues.\textsuperscript{212} As a result of the “substantive changes,” the DHS Notice impacted the following aspects of the way the Privacy Act applies to the system of records, titled, “DHS/USCIS/ICE/CBP001 Alien File, Index, and National File Tracking System of Records”: (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”\textsuperscript{213} of the system of records; and (3) the exemptions claimed under the Privacy Act.\textsuperscript{214} 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

   \begin{itemize}
   \item[(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;
   \item[(6)] add and describe the purpose of the USCIS ELIS, EDMS, and Microfilm Digitization Application System (MiDAS);
   \item[(7)] expand data elements used to retrieve records;
   \item[(8)] update the parameters for retention and disposal of paper A-Files and electronic A-Files;
   \item[(9)] include the MiDAS retention schedule;
   \item[(10)] change system manager to Associate Director, Immigration Records and Identity Services (IRIS);
   \item[(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
   \item[(12)] update routine use E to comply with Office of Management and Budget Circular A-108.
   \end{itemize}

\textit{Id.}\textsuperscript{211} \textit{Id.} at 43,557 (referring to “substantive changes” in the instances of (2) (data storage) and (3) (system location)).

\textsuperscript{211} See supra notes 60–65; see infra discussion in Conclusion.

\textsuperscript{212} See 5 U.S.C. § 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”).

\textsuperscript{213} Privacy Act of 1974, 82 Fed. Reg. at 43,556.
(a) Categories of Records and Sources of Information

One of the “substantive changes” in the Notice is that DHS has “expanded the categories of records.”\textsuperscript{215} 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.”\textsuperscript{216}

Under the Privacy Act, the required notice to a revision of a system of records must include the “categories of sources” for the system.\textsuperscript{217} 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 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.\textsuperscript{218}

The Notice updated 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.”\textsuperscript{219} It is unclear how these sources will be used or what the impact will be.

As discussed above, the Notice broadened the categories of information collected to include “social media handles, aliases, associated identifiable information, and search results.”\textsuperscript{220} However, as one commenter points out “‘social media’” is not defined, and

\textsuperscript{215} Id. at 43,557.
\textsuperscript{216} 5 U.S.C. § 552a(e)(4)(C).
\textsuperscript{217} Id. at § 552a(e)(4)(I).
\textsuperscript{218} Privacy Act of 1974, 82 Fed. Reg. at 43,561.
\textsuperscript{219} Id. at 43,558.
\textsuperscript{220} Id. at 43,557.
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.”

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. 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. In the September 21, 2017, Federal Register Notice, 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, or other federal, state, or local agencies.”

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. 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

---

221 Coalition Letter, supra note 50.
222 See Sharma, supra note 194; Patel & Panduranga, supra note 197; Coalition Letter, supra note 50; Duarte, supra note 210; Scott, supra note 56; Sellars, supra note 142.
223 See Biddle & Woodman, supra note X; Woodman, supra note X (quoting Edward Hasbrouck, Identity Project, explaining that, “AFI is the black-box system of profiling algorithms[,]”).
224 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.”).
225 DHS PIA AFI, supra note X.
social media) or traditional news media, into projects or final intelligence products.”

The AFI system operates efficiently by using data from multiple systems of records. 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.”

In a March 2019 update to the AFI Privacy Impact Assessment, DHS provided two appendices: Appendix A, “Approved AFI External Users (non-CBP Users),” and Appendix B, “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. In Appendix B, DHS states CBP-related data in AFI’s associated system of records and other system interfaces includes 26 additional systems.

Appendix B further elaborates that the “AFI

---

226 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.’”).
227 Id. at 1.
229 DHS PIA AFI, supra note X (announcing March 2019 update on DHS website).
230 Id. at 20-22.
231 Id. at 23-29.
232 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.).
233 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] JO04 Land Border Secondary; TECS IO25
and CIRS” (CPB Intelligence Records System) system of records include an additional 15 systems and databases that are ICE-affiliated;\(^\text{234}\) five systems and databases that are USCIS-affiliated;\(^\text{235}\) one system that is TSA-affiliated;\(^\text{236}\) one system that is Cybersecurity and Infrastructure Security Agency (CISA);\(^\text{237}\) and ten other systems that are inclusive of other governmental or commercial data.\(^\text{238}\)

---

Airport Secondary; IECS IOIL Incident Log; TECS Primary Crossing Person (Primary Query); TECS 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).

\(^\text{234}\) 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 (Deprecating); 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).

\(^\text{235}\) 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)).

\(^\text{236}\) Id. (a database affiliated with TSA includes Secure Flight Passenger Data (SFPB)).

\(^\text{237}\) Id. at 26-27 (a database affiliated with CISA includes Automated Biometric Identification System (IDENT)).

\(^\text{238}\) 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.
AFI and social media data collection that facilitates automated database matching to identify individuals appear to implicate the justification for the 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.”

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[.]” Here, at least one commentator 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).

---


240 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[.]


241 See, e.g., Neilson, supra note X, at 5.
The CMPPA is limited in its reach. In the Federal Register Notice published on June 19, 1989, promulgating Final Guidance in the implementation of CMPPA, the guidance 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

242 The Privacy Act states that the definition of the term “matching program” does not include matches conducted:

(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;
   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.[]

5 U.S.C. § 552a(a)(8)(B)(i-x) (internal citation omitted).
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.244

(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.245 The DHS Notice introduced 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 requestor cooperation.246 The Notice does not make clear to what extent 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.247

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

244 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., Privacy Act of 1974; Final Guidance Interpreting the CMPPA, 54 Fed. Reg. 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[.]”).
247 Neilson, supra note X, at 4.
the federal agency can claim that the disclosure of the record meets certain “conditions of disclosure.”

248 5 U.S.C. § 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 course of the performance of the duties of the Government Accountability Office;
(11) pursuant to the order of a court of competent jurisdiction; or
disclosure is a “routine use” of the record. 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.”

DHS’s Notice stated that it was making several modifications to the databases’ “routine uses” but the Notice did not specify precisely what the modifications were. Under the Privacy Act, the government may disclose to other individuals or agencies the information it has stored on a person without that person’s consent when the sharing of that information is simply compatible with the purposes the information was originally collected for. This allowance for disclosure under the “routine use” condition of the Privacy Act can allow for a broad expansion over time of the entities to which an individual’s collected records may be disclosed.

When DHS published the Notice, “Privacy Act of 1974; System of Records,” on September 18, 2017, DHS specified 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 2017 DHS Notice stated that routine use E was being updated to comply with new policy set forth by the Office of Management and Budget (OMB). It did not specify what changes were made but did provide an updated list of all routine uses pursuant to the Privacy Act. While only E was mentioned, the DHS Notice also made substantive changes to G and K. In contrast, the previous time DHS changed the routine uses they added

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

249 Id. at § 552a(b)(3).
250 Id. at § 552a(e)(4)(D).
252 Neilson, supra note X, at 3.
253 5 U.S.C. § 552a(b)(3).
five new uses, modified eight more and provided a summary of what changes were being made and why they were being made.\textsuperscript{258}

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—that it has compiled on an individual.\textsuperscript{259} In contrast to conditions of disclosure, certain exemptions allow DHS to prevent an individual from being able to access the records that DHS has on him or her.\textsuperscript{260} 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[.]”\textsuperscript{261}

The Federal Register Notice provides that the Privacy Act exemptions are divided into two categories. The first category is characterized as “[g]eneral exemptions”,\textsuperscript{262} and pertains to the law enforcement exemption.\textsuperscript{263} The second category pertains to

\textsuperscript{258} Privacy Act of 1974; DHS—001 Alien File, Index, and NFTSR, 78 Fed. Reg. at 69,864.
\textsuperscript{259} See, e.g., 5 U.S.C. § 552a(b)(1-12).
\textsuperscript{261} DHS claims it is exempt from 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[ ]” and 5 U.S.C. § 552a(f): Author 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[.]

\textsuperscript{262} Id. at § 552a(j).
\textsuperscript{263} Id. at § 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: maintained by an agency or component thereof which performs as its principal function any activity pertaining to the
“[s]pecific exemptions.” Here, the Notice specifically claims exemptions under 5 U.S.C. § 552a(k)(1) and (k)(2), which allow the head of a federal agency to promulgate rules of exemption from any system of records held by the agency under certain provisions. 

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.

Id.

Id. at § 552a(k).

See id. at §552a(k)(1-2):

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[.] See also Appendix C.
DHS exempted their systems 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). 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. 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. The Notice claims a wide range of exemptions as allowed by the Privacy Act, mostly relying on exemptions reserved for criminal law enforcement agencies.

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. DHS will also claim any additional exemptions that are attached to the original system of records.

DHS also claimed “specific exemptions” under subsections (k)(1) and (k)(2). The exemption that DHS claimed under (k)(1)
relates to 5 U.S.C. § 552(b)(1) which grants exemptions to the Freedom of Information Act (FOIA), allowing an agency to withhold information when the information is related to national defense or foreign policy interests and has been classified by Executive Order. The specific exemption under (k)(2) allows an agency to withhold information it has collected on an individual for law

[273] 5 U.S.C. § 552a(k)(1) (“subject to the provisions of section 552(b)(1) of this title[.].”) See also Appendix C.

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[.]


There are nine exemptions to the Freedom of Information Act; each allows agencies to withhold specific types of information.

Exemption 1 covers information “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.” 5 U.S.C. § 552 (b)(1).

The types of information that may be withheld under Exemption 1, pursuant to Executive Order 13526, signed by President Barack Obama on December 29, 2009, are:
Military plans, weapons systems or operations
Foreign government information
Intelligence activities (including covert action), intelligence sources or methods, or cryptology
Foreign relations or foreign activities of the United States, including confidential sources
Scientific, technological or economic matters relating to the national security
U.S. Government programs for safeguarding nuclear materials or facilities
Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to the national security
The development, production or use of weapons of mass destruction[.]

Id.
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. 275 Many of the provisions that DHS has claimed exemptions from under (k)(1) and (k)(2) are also encompassed in (j)(2). 276

B. Undermining Trust in the Privacy Act: DHS Misuse of Privacy Act’s Exemptions

DHS’s recent exemption claims under the Privacy Act’s system of records 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 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.” 277 In October 2008, DHS claimed exemptions from the Privacy Act for Grievances, Appeals, and Disciplinary Action. 278 In December 2008, DHS claimed an exemption of non-criminal investigative information. 279

275 5 U.S.C. § 552a(k)(2). See also Appendix C.
276 Compare Appendix B and Appendix D.
277 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).
For instance, DHS announced that it would maintain a record system to record individuals involved in international trade.\textsuperscript{280}

On January 25, 2017, Privacy Act protections were eliminated for individuals who were not U.S. citizens or Lawful Permanent Residents.\textsuperscript{282} 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.\textsuperscript{283}

On May 4, 2017, DHS invoked the law enforcement exemption of the Privacy Act that then limited access to the FALCON database system of records.\textsuperscript{284} As discussed above, the FALCON Search and

\textsuperscript{280} Privacy Act of 1974: Implementation of Exemptions; DHS/DBP—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).


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. The Privacy Act’s exemption for law enforcement activity allows for DHS to claim that the FALCON tool is part of the federal agency’s law enforcement mission.\(^{285}\)

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 claim protection under the Privacy Act from frustrating the operations of DHS. For instance, on June 14, 2017, DHS published a Federal Register notice that claimed law enforcement exemption for the protection of property of the DHS system of records.\(^{286}\) On July 17, 2017, DHS claimed exemption of “Notice of Arrival and Departure System of Records.”\(^{287}\) On July 27, 2017, DHS published a federal register notice claiming law enforcement exemption of all “Foreign Access Management System of Records.”\(^{288}\)

In response to the “Notice of Modified Privacy Act System of Records” that was published on September 18, 2017, one comment submitted to DHS on October 20, 2017, explained that: “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.”\(^{289}\) DHS claims multiple exemptions, including the

\(^{285}\) *Id.*


\(^{287}\) 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.”).


\(^{289}\) Neilson, *supra* note X, at 5 n.8.
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].”\textsuperscript{290} 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.”\textsuperscript{291} The use of the law enforcement exemption further raises concerns that the accuracy of the algorithms or data analysis used cannot be accessed and checked for inaccuracies by the individual.\textsuperscript{292}

The legislative history reveals that Congress intended the Privacy Act’s exemptions should be kept to an “absolute minimum.”\textsuperscript{293} Exemptions 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.”\textsuperscript{294} Allowing exemptions only in these scenarios encourages government accountability, efficient government operations, and a “public sense of social justice.”\textsuperscript{295} 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.\textsuperscript{296}

\textsuperscript{290} Id.
\textsuperscript{291} 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).
\textsuperscript{292} Social Media Monitoring Report supra note 22, 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.”).
\textsuperscript{293} Privacy Act of 1974, Reports, 93\textsuperscript{rd} Congress, 93-1183, supra note 25, at 20.
\textsuperscript{294} Id. at 21.
\textsuperscript{295} Id.
\textsuperscript{296} 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)).
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.”297 The Committee noted that the government should refrain “from compulsory data collection” systems to respect the freedom and privacy interests of the citizenry.298 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.”299 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.”300

Congress was clear 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 justice purposes[.]”301 Even for agencies that fall under the exemptions, the federal agencies must publish in the Federal Register

297 Id. at 74.
298 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)).
299 Id. at 74.
300 Id.
“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.”

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.” Exemptions should only apply when societal interests overwhelmingly outweigh individual privacy. 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 investigation, 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.” “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.”

CONCLUSION

The relationship between citizen and state is rapidly changing in profound ways in the digital age. This is a direct consequence of a rapidly evolving digital economy that privacy experts such as

---

302 Id. at 4.
303 Id. at 37.
304 Id.
305 Id.
306 Id. at 38.
307 See generally COHEN, supra note 4; CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE (Jeffrey Rosen & Benjamin Wittes eds., 2011); DONOHUE, FUTURE OF FOREIGN INTELLIGENCE, supra note 10; GRANICK, supra note 9; 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).
Shoshana Zuboff describe as a surveillance economy and surveillance capitalism and what Julie Cohen has referred to as the surveillance-innovation complex. 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.”

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

308 Zuboff, supra note 1, at 94; 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).
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 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. Further, widespread social media surveillance practices across multiple agencies have been underway for nearly a decade. Social media surveillance programs by federal agencies are largely unregulated and the announcement of social media collection 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, 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. Congress observed that the technological

---


314 See generally id. app. at 35-36.

315 Privacy Act of 1974, Reports, 93rd Congress, 93-1416, supra note X, at 3.
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.”

Passage of the Privacy Act was meant to engender trust. Trust in the Privacy Act is at risk when the Act’s required notice announces the expansion of new 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.

316 Id.
Appendix A

Privacy Act’s General Exemptions: Definitions

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


<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(c)(3)</td>
<td>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[.].</td>
</tr>
<tr>
<td>(c)(4)</td>
<td>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.</td>
</tr>
<tr>
<td>(d)</td>
<td>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...</td>
</tr>
</tbody>
</table>
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.”

(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—
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

Privacy Act’s Specific Exemptions: Definitions

### 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 (l) 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 (l) 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

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

<table>
<thead>
<tr>
<th>5 U.S.C. § 552a</th>
<th>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)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(c)(3)</td>
<td>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[,]</td>
</tr>
<tr>
<td>(d)</td>
<td>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</td>
</tr>
</tbody>
</table>
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.