WASHINGTON
LEGISLATIVE OFFICE

February 28, 2017

Donald F. McGahn
Assistant to the President and White House Counsel
1600 Pennsylvania Ave. NW, 2nd Floor, West Wing
Washington, D.C. 20500

Re: Privacy Implications of Executive Order 13768: Enhancing Public Safety in the Interior of the United States

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

FAIZ SHAKIR
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

Dear Mr. McGahn,

In recent weeks, President Trump has issued several executive orders that represent an attack on the rights of immigrants and foreigners—including the right to privacy that has been protected for decades in prior Republican and Democratic administrations. Specifically, Section 14 of President Trump's Executive Order 13768, signed January 25, 2017, and entitled "Enhancing Public Safety in the Interior of the United States ("Section 14" or the "EO") states that: "[a]gencies shall, *to the extent consistent with applicable law*, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information" (emphasis added).[1] This dramatic shift in policy will create an implementation nightmare that threatens the privacy rights of immigrants, foreign residents, and U.S. citizens; raises multiple constitutional and legal concerns; and calls into question whether the U.S. is meeting its obligations under existing international agreements. Thus, we urge you to swiftly reverse this policy change and recognize that it cannot be achieved "consistent with applicable law."

However, should the administration attempt to implement this unwise and flawed policy, it is critical to understand that existing law limits how agencies may implement such changes in multiple, significant ways. Specifically, as discussed in detail below, prior to making changes to existing privacy protections applied to so-called mixed systems of records that contain the information of citizens and lawful permanent residents (collectively, "U.S. persons") as well as other noncitizens, federal law mandates that agencies must, at a minimum:

1. Issue an amended system of records notice ("SORN"), requiring a 30-day minimum comment period, for any mixed system that was granted Privacy Act protections prior to issuance of the EO;

[1] Exec. Order No. 13,768, 82 Fed. Reg. 8,799 (Jan. 25, 2017), *available at* https://www.gpo.gov/fdsys/pkg/FR-2017-01-30/pdf/2017-02102.pdf.

2. Conduct a privacy impact assessment of mixed systems of records previously granted Privacy Act protections that examines the risk that U.S. and non-U.S. persons will have their rights violated and that identifies procedures to promptly provide Privacy Act protections to people who change their status to lawful permanent resident or U.S. citizen;
3. Put in place procedures to address the constitutional and statutory obligations of the government to limit the collection and dissemination of individuals' private information and provide access to agency records; and
4. Ensure that any changes are consistent with U.S. obligations under existing international agreements.

Based on publicly circulated versions of implementation memos, it appears that some federal agencies intend to implement Section 14 without taking the steps cited above.[2] Specifically, it appears that the Department of Homeland Security intends to simply revoke its existing policy, without assessing and making the changes necessary to ensure that the rights of citizens, lawful permanent residents, other immigrants, and foreign residents are adequately protected. Any attempt by an agency to make changes to the protections provided to mixed systems of records without complying with the steps outlined above, will be in violation of the law. Given these concerns, we request the opportunity to meet with you regarding how you plan to implement Section 14, and to discuss the privacy and civil liberties interests at stake.

I. Background

The Privacy Act of 1974 (the "Act") requires that the federal government adhere to certain fair information practices in collecting, maintaining, using, and sharing the personal information of individuals.[3] The Act applies to any "system of records," which is defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[4] The Act controls when federal agencies can collect personal information and when and how they can disclose records containing that information; it allows individuals to access and correct their own records; and it requires agencies to notify people about the systems of records and to ensure the systems' security and accuracy.[5]

---

[2] Memorandum from John Kelly, Sec., Dept. of Homeland Security, Enforcement of the Immigration Laws to Serve the National Interest (Feb. 20, 2017), *available at* https://www.dhs.gov/sites/default/files/publications/17_0220_S1_Enforcement-of-the-Immigration-Laws-to-Serve-the-National-Interest.pdf ; Memorandum from John Kelly, Sec., Dept. of Homeland Security, Implementing the President's Border Security and Immigration Enforcement Improvements Policies (Feb. 20, 2017), *available at* https://www.dhs.gov/sites/default/files/publications/17_0220_S1_Implementing-the-Presidents-Border-Security-Immigration-Enforcement-Improvement-Policies.pdf;

[3] Privacy Act of 1974, 5 U.S.C. § 552(a).

[4] *Id.* at § 552a(a)(5).

[5] *See* 5 U.S.C. § 552a. While the ACLU has testified before Congress that the Privacy Act needs to be updated to better protect privacy rights in the digital age, it nonetheless provides an important framework for government use of personally identifiable information. *See State of Federal Privacy and Data Security Law: Lagging Behind the Times? Before the S. Comm. On Homeland Security and Gov't. Affairs Subcomm. On Oversight of Gov't.Mgmt.the Fed. Workforce and the D.C.*112th Cong. (2012) (statement of Christopher R. Calabrese, Legislative Counsel, A.C.L.U.), *available at* www.hsgac.senate.gov/download/?id=ac5e64f7-0167-44bc-9359-ef504f4b7bc2.

The Privacy Act generally applies when federal agencies collect information about U.S. citizens and lawful permanent residents (or "U.S. persons"), and it has historically also been applied to "mixed systems" of records, which contain information about both U.S. and non-U.S. persons. Since 1975, one year after Congress passed the Privacy Act, the Office of Management and Budget has encouraged agencies to treat mixed systems "as if they were, in their entirety, subject to the Act."[6] Accordingly, agencies including the Department of Health and Human Services,[7] the Department of Justice, the State Department, and the Department of Homeland Security[8] apply Privacy Act protections to all records held in mixed systems regardless of the immigration status of the individual. Agencies have noted that adoption of such a policy has the benefit of supporting data integrity, advancing cross-border information sharing, facilitating trade and travel, encouraging protection of U.S. persons' privacy overseas, and creating consistency with provisions in the E-Government Act of 2002.[9]

II. Legal Constraints on Implementation of the Executive Order

Under federal law, federal agencies cannot implement the Executive Order unless they first take the following steps: issue a system of records notice ("SORN") for any mixed system that is currently entirely covered by the fair information practices of the Privacy Act; conduct a privacy impact assessment of every such system that collects, maintains, or disseminates the information of non-U.S. persons; and put in place rules to address the constitutional limits on the government's ability to collect and disseminate individuals' private information. Agencies must additionally ensure that any changes to existing practices are consistent with assurances underpinning international agreements currently in force, including the E.U.-U.S. Agreement on Data Protection in the cases of Exchanges of Personal Data for Law Enforcement Purposes (the "Umbrella Agreement") and the Privacy Shield.

A. Any federal agency applying Section 14 of the Executive Order to a mixed system that is currently entirely covered by the fair information practices of the Privacy Act must publish a System of Records Notice and provide a 30-day comment period.

Federal law provides that any agency that currently applies the fair information practices of the Privacy Act to a mixed system of records must publish an amended SORN in the Federal Register and provide a 30-day comment period for that SORN before the agency can implement Section 14. The Privacy Act requires that federal agencies amend a SORN, which is subject to notice and comment, whenever they make a "significant alteration" to an existing system of records. Any attempt to implement Section 14 will necessarily result in significant alterations—which the federal government defines as changes "in the manner in which the records are

---

[6] Privacy Act Implementation; Guidelines and Responsibilities, 40 Fed. Reg. 28,948 (July 9, 1975), *available at* https://web.archive.org/web/20151019030714/https:/www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf.

[7] *See* Privacy Act of 1974; System of Records Notice, 81 Fed. Reg. 46,682 (July 18, 2016), *available at* https://www.gpo.gov/fdsys/pkg/FR-2016-07-18/pdf/2016-16812.pdf.

[8] *See* Memorandum from Hugo Teufel III, Chief Privacy Officer, Dept. of Homeland Security, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-US Persons (Jan. 7, 2009), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

[9] *Id.* at 4-6.

organized, indexed, or retrieved that results in a change in the nature or scope of these records," changes "in the purpose for which information in the system of records is used," and changes "in procedures associated with the system in a manner that affects an individual's exercise of his or her rights."[10] Because implementing Section 14 will require federal agencies to differentiate non-U.S. persons' information from U.S. persons' information in mixed systems, the agencies will have to change the manner in which their records are organized or retrieved and the procedures they use to determine which individuals are subject to the Act. These significant alterations cannot be made without a new SORN and its requisite comment period.

B. Before collecting new information about non-U.S. persons or altering the treatment of existing mixed systems, federal agencies must conduct privacy impact assessments.

Pursuant to Section 208 of the E-Government Act of 2002, federal agencies must conduct privacy impact assessments before collecting new personally identifiable information about non-U.S. persons and before altering any existing mixed system that extends Privacy Act protections regardless of immigration status.[11] As the Department of Homeland Security ("DHS") recognized in its Privacy Policy Guidance Memorandum, issued during the Bush Administration, the E-Government Act "does not limit its coverage only to U.S. persons" and "requires that privacy impact assessments be conducted on all new Federal systems collecting information in identifiable form and on any existing Federal systems that are making major changes, collecting new types of information, or changing system uses." The DHS Guidance notes that the E-Government Act "requires that an information system be analyzed for privacy risks based on the architecture of the system itself and its associated collections and uses, without regard to whom the system covers."[12]

Federal agencies therefore cannot implement Section 14 of the Executive Order without conducting a privacy impact assessment on any mixed system of records that stands to lose Privacy Act protections, or any system for which the agencies will collect personally identifiable information differently in the future. Such privacy impact assessments must specifically address the risk that U.S. persons and others who are entitled to privacy protections through international agreements will have their rights violated due to their private information being included in a mixed system of records that is not fully covered by the Privacy Act. It must also identify procedures for promptly providing Privacy Act protections to individuals who become lawful permanent residents or U.S. citizens and whose personally identifying information is maintained by the federal agency.

---

[10] *See* CHIEF INFORMATION OFFICER, SYSTEM OF RECORDS NOTICE (SORN) GUIDE (U.S. Off. of Personnel Mgmt., 2010), *available at* https://www.opm.gov/information-management/privacy-policy/privacy-references/sornguide.pdf.

[11] *See* E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. (2002); 44 U.S.C. Ch. 36.

[12] Memorandum from Hugo Teufel III, *supra* note 8.

C. Federal agencies must put in place procedures to address the constitutional and statutory limits affecting the treatment of non-U.S. persons' sensitive personal information.

The constitutional right to informational privacy places important limitations on the disclosure of sensitive personal information held in government databases. As courts have repeatedly made clear, the Fifth Amendment's Due Process Clause prohibits government collection of sensitive personal information without sufficient safeguards against privacy violations. "Even if a law adequately protects against *public* disclosure of a [person's] private information, it may still violate informational privacy rights if an unbounded, large number of government employees have access to the information."[13]

The Supreme Court has explained that the protections of the Privacy Act, including its limits on agencies sharing records with other government agencies, are crucial to the reasonableness of federal data collection. In *NASA v. Nelson*,[14] the Court held that the government's collection of information about federal employees' drug use did not violate a constitutional right to informational privacy "[i]n light of the protection provided by the Privacy Act's nondisclosure requirement." Without the Privacy Act or a similar "statutory or regulatory duty to avoid unwarranted disclosures,"[15] the government's collection and retention of the data would raise serious constitutional concerns.

In certain contexts, courts have recognized that the government has a constitutional obligation to provide individuals access to their agency records. For example, in immigration proceedings, the U.S. Court of Appeals for the Ninth Circuit has ruled that the government has a constitutional obligation to furnish copies of an individuals' A-file at their request.[16] Thus, any new procedures that agencies adopt that limit individuals' access to agency records must be consistent with the government's constitutional obligations in this arena.

Furthermore, other federal laws, including the Violence Against Women Act, include confidentiality provisions that limit the dissemination of the personally identifying information of noncitizens that have been the victims of violence.[17] Changes to systems of records must ensure compliance with these laws. For example, should agencies decide to go forward with implementing Section 14, they must put in place alternative procedures that restrict dissemination consistent with the requirements in the Violence Against Women Act.

Removing Privacy Act protections from sensitive records in federal databases can leave those records open to unjustified sharing with other agencies and potentially unconstrained public dissemination. To avoid violating constitutional and legal privacy protections, agencies must either continue to apply the Privacy Act fair information practices to systems of records containing non-U.S. persons' data, or adopt policies implementing equivalent protections.

---

[13] Tucson Woman's Clinic v. Eden, 379 F.3d 531, 551–52 (9th Cir. 2004).
[14] NASA v. Nelson, 562 U.S. 134, 159 (2011).
[15] *Id.* at 155.
[16] Dent v. Holder, 627 F.3d 365, 374-75 (9th Cir. 2010).
[17] *See, e.g.*, 8 U.S.C. § 1367(a)(2).

D. International agreements such as the E.U.-U.S. Umbrella Agreement restrict the ability of federal agencies to withhold privacy protections from all non-U.S. persons.

Implementation of Section 14, without adoption of additional protections, may also undermine existing international agreements. These agreements include the Privacy Shield, which provides a framework enabling the commercial exchange of data between U.S. and European companies in a manner consistent with E.U. privacy laws, and the E.U.-U.S. Umbrella Agreement, which is an agreement between the U.S. government and the European Union to allow data sharing among their law enforcement authorities. For example, the Privacy Shield framework's adequacy under the E.U. Charter of Fundamental Rights relied in part on the U.S. government's assurance that there were appropriate mechanisms in place for individuals to seek redress in cases where their data was accessed by the U.S. government.[18] Similarly, the Umbrella Agreement requires the U.S. to ensure that E.U. residents are entitled to access and correct their personal information, unless specified exceptions apply.[19] The Umbrella Agreement also requires that the U.S. provide the ability to seek administrative redress to individuals in the E.U. in cases where they are improperly denied the ability to access or correct their information.[20] Under these agreements, U.S. citizens are also provided reciprocal privacy protections.

Implementation of Section 14 must include adoption of policies that are consistent with the U.S. prior assurances in this arena. Though implementation of the Judicial Redress Act, which was passed as a precondition to entering into the Umbrella Agreement, provides a measure of privacy protection for citizens of E.U. countries, such protections do not provide the full range of protections that were afforded under the Privacy Act. Specifically, the Judicial Redress Act does not protect residents of the E.U. who are not citizens, provide redress in cases where privacy violations involving dissemination were not willful or intentional, and does not apply to non-designated agencies. Implementation of Section 14 must consider these deficiencies, and whether alternative protections are required for the U.S. to be in compliance with its obligations under the Privacy Shield and Umbrella Agreement.

The need to provide additional protections consistent with these agreements and the Judicial Redress Act further complicates implementation of Section 14. Mixed systems of records held by federal agencies cannot simply be segregated for purposes of privacy protections based on an individual's status as a U.S. person—they must also include an analysis of whether the individual is a citizen of a country who may be entitled to enhanced protection by virtue of the Judicial Redress Act or other obligations under existing international agreements. For this reason, privacy impact assessments conducted by federal agencies must specifically account for the Privacy Shield and the Umbrella Agreement (including implementation of the Judicial Redress Act), and must address the ways in which mixed systems will continue to protect the privacy rights of individuals covered by these agreements.

---

[18] Comm'n Implementing Decision (EU) No. 2016/1250, 2016 O.J. (L. 207/1) ¶ 25, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN.

[19] Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses (draft 2016) at articles 16 and 17, *available at* http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.

[20] *Id*. article 18.

III. Implementation of Section 14 is impractical and will cost millions of dollars with no resulting benefit.

In addition to the legal constraints to implementation, federal agencies should also consider the substantial practical pitfalls inherent in implementing Section 14 of the EO. Agencies have openly recognized these pitfalls in the past. During the Bush Administration, for example, DHS noted that "[a]n agency treats mixed systems as Privacy Act systems, in part, because of inherent difficulties in determining an individual's current citizenship status, which may change over time through naturalization or adjustment."[21]

Beyond the fact that an individual's status may change over time, many types of records contain information about multiple individuals, some of whom may be U.S. persons (citizens or lawful permanent residents), and some of whom may be non-U.S. persons. For example, only U.S. citizens and lawful permanent residents may file a Petition for an Alien Relative, and records relating to such petitions will obviously combine information not only about the petitioner, but about the noncitizen beneficiary as well.

Now, those difficulties are even more significant given the E.U.-U.S. Umbrella Agreement and the Judicial Redress Act, which bring millions of individuals from European countries within the ambit of required privacy protections. As a result, federal agencies cannot simply rely on the fact that an individual is a non-U.S. person—which is itself complicated by changes in status over time—to determine how that individual's information is treated. These intricacies highlight the fact that Section 14 of the EO is not only a privacy threat, but is also an administrative nightmare that will cost millions of dollars to implement.

The federal government currently has millions, if not billions, of records in existing mixed systems. Implementing the EO will require federal agencies to go through a time- and resource-intensive, multi-step process to determine what privacy protections should apply to each of these records. First, agencies will have to examine each record individually to determine what personally identifiable information ("PII") it contains. This step alone will be complicated by the fact that in many cases, as noted, a single record will identify multiple individuals with varying nationalities and immigration statuses. Once the agency has identified what PII the record contains, it will then need to determine the identified individual's current immigration status, which may not be readily apparent and may therefore require additional investigation by the agency. Finally, for all non-U.S. persons, the agency will then need to determine if the individual is covered by the Judicial Redress Act and therefore protected by some, though not all, Privacy Act provisions.

An example from the State Department demonstrates just how unworkable this process will be for federal agencies. The Consular Consolidated Database is a mixed database with over 143 million records, some dating back to the mid-1990s.[22] Even assuming that the State Department needs only 2 minutes to accurately determine what Privacy Act protections should apply to each

[21] Memorandum from Hugo Teufel III, *supra* note 8.
[22] RUTH ELLEN WASEM, IMMIGRATION: VISA SECURITY POLICIES, (Cong. Research Service, 2015), *available at* https://fas.org/sgp/crs/homesec/R43589.pdf.

record—a drastic underestimate—it would take over 2,200 federal employees working 40 hours a week for 52 weeks to implement Section 14 of the EO just for that single database. Given the current federal hiring freeze, such workers would need to be re-allocated from other job functions.

In addition to creating an administrative nightmare, implementing Section 14 of the EO would also inevitably lead to errors that would deprive U.S. persons, nonimmigrants, and foreign residents of privacy protections they are entitled to by law. Existing federal databases already contain numerous errors that have led to U.S. persons losing out on a job opportunity due to incorrect information regarding their immigration status. For example, the Government Accountability Office has found that, despite efforts to institute quality control measures, the e-Verify system remains error-ridden.[23] According to estimates drawn directly from DHS, in FY 2009, at least 80,000 American workers lost out on a new job because of a mistake in the government database.[24]

Given the prevalence of errors regarding immigration status in existing federal databases, it is highly likely that any attempt to deprive non-U.S. persons' of protections under the Privacy Act will result in similar, if not more egregious, errors. If a federal agency is collecting or disseminating personally identifiable information based on incorrect information about a person's immigration status, doing so could result in that person's privacy rights being violated. Any such errors will disproportionately impact lawful immigrants and naturalized citizens, given that their immigration status can change over time and, therefore, so may the treatment of their personally identifiable information.

For all of the legal and practical considerations outlined above, federal agencies should continue to extend the fair information practices of the Privacy Act to mixed systems of records in their entirety.

Sincerely,

Faiz Shakir
Director

Esha Bhandari
Staff Attorney

[23] U.S. GOV'T ACCOUNTABILITY OFF., REPORT TO THE SUBCOMMITTEE ON SOCIAL SECURITY, COMMITTEE ON WAYS AND MEANS, HOUSE OF REPRESENTATIVES, EMPLOYMENT VERIFICATION: FEDERAL AGENCIES HAVE TAKEN STEPS TO IMPROVE E-VERIFY, BUT SIGNIFICANT CHALLENGES REMAIN (2010), *available at* http://www.gao.gov/new.items/d11146.pdf.

[24] *Hearing on the Social Security Administration's Role in Verifying Employment Eligibility Before the H. Comm. On ways and Means Subcomm. On Social Security*, 112th Cong. 2 (2011) (statement of Tyler Moran, Policy Dir., Nat'l Immigration law Ctr.), *available at* https://www.nilc.org/wp-content/uploads/2015/12/SSA-subcommittee-Moran-testimony-4-14-11.pdf.

Neema Singh Guliani
Legislative Counsel

CC:
Michael L. "Mike" Young, Secretary (Acting)
Department of Agriculture

Kelvin Fairfax, Chief Privacy Officer
Department of Agriculture

Wilbur L. Ross, Jr., Secretary
Department of Commerce

Catrina Purvis, Chief Privacy Officer and Director of Open Government
Department of Commerce

Gen James N. "Jim" Mattis, USMC (Ret), Secretary
Department of Defense

Cindy L. Allard, Director, Defense Privacy and Civil liberties Office
Department of Defense

Elisabeth Prince "Betsy" DeVos, Secretary
Department of Education

Kathleen M. Styles, Chief Privacy Officer and Director
Department of Education

Dr. Grace M. Bochenek, Secretary (Acting)
Department of Energy

Jerry Hanley, Chief Privacy Officer
Department of Energy

Thomas Edmunds "Tom" Price, Secretary
Department of Health and Human Services

Robinsue Frohboese, Director (Acting), Office for Civil Rights
Department of Health and Human Services

Gen John F. Kelly, USMC (Ret), Secretary
Department of Homeland Security
Jonathan R. Cantor, Chief Privacy Officer (Acting)
Department of Homeland Security

Craig T. Clemmensen, Secretary (Acting)
Department of Housing and Urban Development

Ruby B. Porch, Privacy Act Officer (Acting)
Department of Housing and Urban Development

K. Jack Haugrud, Secretary (Acting)
Department of the Interior

Sylvia Burns, Chief Information Officer
Department of the Interior

Jefferson "Jeff" Sessions, III, Attorney General
Department of Justice

Peter Winn, Director, Office of Privacy and Civil Liberties
Department of Justice

Edward C. Hugler, Secretary (Acting)
Department of Labor

Nicholas Christopher "Nick" Geale, Solicitor (Acting)
Department of Labor

Rex W. Tillerson, Secretary
Department of State

Christina Jones-Mims, Privacy Division Chief
Department of State

Steven Terner Mnuchin, Secretary
Department of the Treasury

Timothy Skinner, Director, Office of Privacy and Civil Liberties
Department of the Treasury

Elaine L. Chao, Secretary
Department of Transportation

Kristen Baldwin, Chief Information Officer (Acting)
Department of Transportation

John Michael "Mick" Mulvaney, Director
Office of Management and Budget

Dr. David J. Shulkin, MD, Secretary
Department of Veterans Affairs

F. John Buck, Jr., Director, Office of Privacy and Records Management
Department of Veterans Affairs

Michael Richard "Mike" Pompeo, Director
Central Intelligence Agency

Benjamin T. Huebner, Privacy and Civil Liberties Officer
Central Intelligence Agency

Michael Dempsey, Director of National Intelligence (Acting)
Office of the Director of National Intelligence

Alexander W. Joel, Civil Liberties Protection Officer
Office of the Director of National Intelligence