October 18, 2017

Jonathan R. Cantor
Acting Chief Privacy Officer
Privacy Office, Department of Homeland Security
Washington, DC 20528-0655

COMMENTS ON A DEPARTMENT OF HOMELAND SECURITY NOTICE OF MODIFIED PRIVACY ACT SYSTEM OF RECORDS REGARDING THE DEPARTMENT OF HOMELAND SECURITY/U.S. CITIZENSHIP AND IMMIGRATION SERVICES, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, U.S. CUSTOMS AND BORDER PROTECTION—001 ALIEN FILE, INDEX, AND NATIONAL FILE TRACKING SYSTEM OF RECORDS

Docket No. DHS-2017-0038

SUBMITTED BY THE NATIONAL IMMIGRATION LAW CENTER

The National Immigration Law Center (NILC) submits the following comments on the Sept. 15, 2017 Notice of Modified Privacy Act System of Records[1] for the Department of Homeland Security/U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, U.S. Customs And Border Protection—001 Alien File, Index, and National File Tracking System of Records.

Established in 1979, the National Immigration Law Center (NILC) is one of the leading organizations in the U.S. exclusively dedicated to defending and advancing the rights of immigrants with low income. Our mission is grounded in the belief that every American—and aspiring American—should have the opportunity to fulfill their full potential regardless of where they were born or how much money they have.

[1] Notice of Modified System of Records, Department of Homeland Security/U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection—001 Alien File, Index, and National File Tracking System of Records (hereafter "the SORN") https://www.gpo.gov/fdsys/pkg/FR-2017-09-18/pdf/2017-19365.pdf

SUMMARY OF COMMENTS

- The System of Records Notice (SORN) improperly expands the official record of an individual's immigration history to include "social media handles and aliases, associated identifiable information, and search results" and improperly expands record source documents to include "information obtained from the Internet, public records, public institutions, interviewees, [and] commercial data aggregators."
- The SORN gives official status to this massive and random collection of information.
- The Department of Homeland Security (DHS) is not transparent about its collection, use, storage, and sharing of such information.
- The SORN authorizes continuous, open-ended monitoring of immigrants and citizens without probable cause or reasonable suspicion of wrongdoing and without transparency, oversight or accountability.
- The notice in effect authorizes the creation of secret files. As a result of exemptions from Privacy Act protections requiring notice of, access to and accuracy of information that has been collected, individuals won't know that they are being monitored, how they are being monitored or that their information has been collected, stored and shared. In addition, the opportunity to correct inaccurate information is either limited or non-existent. Individuals have no recourse to address any harmful consequences.

DESCRIPTION OF CHANGES MADE BY THE SORN

The Sept. 15, 2017 SORN for the Department Of Homeland Security/U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, U.S. Customs And Border Protection—001 Alien File, Index, and National File Tracking System of Records updates a 2013 SORN.[2] Among other things, the new SORN:

- Redefines the "official record of an individual's immigration history" to include a paper Alien File (A-file), the electronic record in the Enterprise Document Management System or USCIS's Electronic Immigration System, or a combination of paper and electronic records and supporting documentation;
- Expands the categories of records to include "social media handles and aliases, associated identifiable information, and search results."
- Updates record source categories to include "information obtained from the Internet, public records, public institutions, interviewees, [and] commercial data aggregators."
- Maintains significant exemptions from Privacy Act protections.

[2] Notice of Modified Privacy Act System of Records (Nov. 21, 2013) https://www.federalregister.gov/documents/2013/11/21/2013-27895/privacy-act-of-1974-department-of-homeland-security-us-citizenship-and-immigration-services-us

UNDER THE SORN, A MASSIVE AND RANDOM COLLECTION OF INFORMATION GATHERED FROM SOCIAL MEDIA, COMMERCIAL DATA AGGREGATORS, AND THE INTERNET BECOMES A PERMANENT PART OF THE OFFICIAL RECORD OF AN INDIVIDUAL'S IMMIGRATION HISTORY.

The SORN specifically lists "social media handles and aliases, associated identifiable information, and search results" to the data elements contained in paper or electronic A-files. In addition, the SORN lists "information obtained from the Internet, public records, public institutions, interviewees, [and] commercial data aggregators" as among the source categories for records in the system.

The SORN thus allows a massive and random collection, storage and use of a vast quantity of information, without limits or standards. Even more disturbingly, this information becomes part of the official record of an individual's immigration history and is accorded the same significance as other information in the file. That history thus has an official status that can be shared with innumerable agencies and governments.

The SORN both acknowledges the official nature of an A-file and understates its use:

> The A-file serves as the official record of an individual's immigration history. It is used in immigration proceedings before U.S. Department of Justice (DOJ) immigration judges and the Board of Immigration Appeals (BIA), and is the official record used in Federal court litigation and other official agency business transactions.[3]

In fact, as the SORN makes clear, an A-file's use as an official record is much broader. The SORN authorizes disclosure of all or a portion of records in the system to a wide variety of governmental, law enforcement, judicial, administrative and other agencies outside of DHS, in addition to the general disclosures permitted under 5 USC 552a(b)[4] of the Privacy Act. Information may be disclosed to federal, state, local and foreign agencies.

According to DHS, A-file records are permanent, and their contents are transferred to the National Archives and Records Administration 100 years after the individual's birth.[5] Once collected, information remains in the individual's A-file forever.

DHS IS NOT TRANSPARENT ABOUT ITS USE OF INFORMATION GATHERED FROM SOCIAL MEDIA, COMMERCIAL DATA AGGREGATORS, AND INFORMATION GLEANED FROM THE INTERNET.

---

[3] SORN, Background, https://www.gpo.gov/fdsys/pkg/FR-2017-09-18/pdf/2017-19365.pdf,
[4] https://www.law.cornell.edu/uscode/text/5/552a
[5] SORN, Policies and Practices for Retention and Disposal of Records, https://www.gpo.gov/fdsys/pkg/FR-2017-09-18/pdf/2017-19365.pdf

DHS has, in fact, collected and used social media since at least 2012.[6] Yet during the intervening years, it did not issue a SORN that described this practice, and did not issue a Privacy Impact Assessment (PIA) detailing any privacy protections related to collection and use of social media.

And DHS is disingenuous now about the impact of the changes made by the SORN. In a September, 2017 email to the online publication Gizmodo, the agency claimed:

> This policy permits a small cadre of specifically trained 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.[7]

But under the SORN, access to an individual's social media is not limited to a "small cadre of specifically trained USCIS officers." And the categories of individuals whose information may be collected, used and shared are broad.[8] Naturalized citizens (not

---

[6] On June 8, 2012 DHS issued an Instruction implementing the Department of Homeland Security (DHS) Directive 110-01, Privacy Policy for Operational Use of Social Media. https://www.dhs.gov/sites/default/files/publications/Instruction_110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf

[7] Matt Novak, "US Homeland Security Says Tracking Social Media of Immigrants is Nothing New," (Gizmodo, 9/28/17) https://gizmodo.com/us-homeland-security-says-tracking-social-media-of-immi-1818875395

[8] The listed categories include lawful permanent residents; naturalized U.S. citizens; individuals when petitioning for benefits under the INA, as amended, on behalf of another individual; individuals acting as legal guardians or designated representatives in immigration proceedings involving an individual who has a physical or developmental disability or mental impairment (as authorized under the INA); individuals who receive benefits under the INA; individuals who are subject to the enforcement provisions of the INA; individuals who are subject to the INA and are under investigation by DHS for possible national security threats or threats to the public safety, were investigated by DHS in the past, are suspected of violating immigration-related criminal or immigration-related civil provisions of treaties, statutes, regulations, Executive Orders, and Presidential Proclamations administered by DHS, or are witnesses and informants having knowledge of such violations; relatives and associates of any of the individuals listed above who are subject to the INA; individuals who have renounced their U.S. citizenship; civil Surgeons who are required to conduct and certify medical examinations for immigration benefits; and law enforcement officers who certify a benefit requestor's cooperation in the investigation or prosecution of a criminal activity; preparers assisting an individual seeking an immigration benefit or agency action under the INA; interpreters assisting an individual seeking an immigration benefit or agency action under the INA; attorneys or representatives recognized by USCIS or accredited by the BIA; or law enforcement officers who certify a benefit requestor's cooperation in the investigation or prosecution of a criminal activity.

simply those applying for citizenship) are specifically included, along with all other non-citizens, whether documented or undocumented. In addition, even DHS' incomplete description of an A-file, as well as the SORN itself, make clear that the A-file will be used for purposes beyond applications for benefits, making explicit that it (and thus information in it from social media) will be used for immigration enforcement and other investigative purposes.

DHS does not define social media in the SORN. Its 2012 instruction regarding operational use of social media defines social media (a definition which has likely evolved since then) as:

> the sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact. Social media take many different forms, including but not limited to web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies.[9]

As is clear even from this definition, a social media search would necessarily include information pertaining to other people. That information would also become part of an individual's permanent official immigration record, but the SORN makes no mention of that inclusion or its impact.

THE NOTICE AUTHORIZES CONTINUOUS, OPEN-ENDED MONITORING OF IMMIGRANTS AND CITIZENS WITHOUT PROBABLE CAUSE OR REASONABLE SUSPICION OF WRONGDOING AND WITHOUT TRANSPARENCY, OVERSIGHT OR ACCOUNTABILITY.

DHS has made clear that it wishes to conduct continuous and wide-ranging monitoring of non-citizens and views the absence of continuous vetting as a significant gap in its ability to identify emerging risks. As DHS recently wrote as part of an event to discuss future contracts for vetting of non-citizens, "the gaps in the current vetting model along with existing limitations in the vetting process create a compelling case for ICE to take action to develop and implement a continuous vetting strategy, framework and process." [10]

---

[9] https://www.dhs.gov/sites/default/files/publications/Instruction_110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf , p. 4.

[10] Attachment 1 to July 6, 2017 ICE-HSI-Data Analysis Service Amendment, https://www.fbo.gov/?s=opportunity&mode=form&id=48b393a8498798f078ab8d29612b5e15&tab=core&_cview=0 According to DHS, "ICE does not perform any regular, periodic or continuous review or vetting of nonimmigrants against screening criteria once they have entered the US. While certain programs perform reviews once certain criteria are met there is no existing process that systematically reviews nonimmigrants once their risk profile has changed. Persons who are on immigrant visas or who have filed for or received immigration benefits (i.e. Green Card, asylum or refugee status) do not receive continuous vetting outside of the benefits adjudication process performed by US Citizenship and Immigration Services (USCIS)…. Moreover, there are many

The information collection, storage and use allowed by the SORN fits within this continuous monitoring strategy, framework and process.

DHS takes a broad view of what it means by monitoring of publicly available information. For example, as part of the recent event exploring future extreme vetting contracts, DHS wrote:

> The Contractor shall analyze and apply techniques to exploit publically 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."[11]

The 2017 SORN's dangerously vague language could permit the collection of this type of publicly available information, but provides no standards such as probable or reasonable cause to limit collection, storage, use and sharing. The inclusion of social media and other publicly available information will undoubtedly have a chilling effect on participation in activities protected y the First Amendment to the Constitution.

Nor does the SORN provide any measure of transparency, oversight or accountability. DHS' track record in pilot programs to use social media is abysmal, with the DHS Inspector General concluding in 2017 that USCIS and ICE pilot projects to use social media for vetting purposes "did not define what would constitute a successful outcome, nor did [DHS] identify metrics against which to benchmark its findings."[12]

AS A RESULT OF EXEMPTIONS FROM PRIVACY ACT PROTECTIONS, INDIVIDUALS WON'T KNOW THAT THEY ARE BEING MONITORED, HOW THEY ARE BEING MONITORED, OR THAT THEIR INFORMATION IS COLLECTED, STORED AND SHARED. THE OPPORTUNITY TO CORRECT INCORRECT INFORMATION IS EITHER LIMITED OR NON-EXISTENT.

---

immigrant and nonimmigrant classes with long periods of validity tied to their benefit or visa class which results in significant time periods passing between vetting reviews. This increases potential risk while further inhibiting ICE's ability to identify emerging risks in an actionable timeframe."

[11] Attachment 2 to July 6, 2017 ICE-HIS-Data Analysis Service Amendment https://www.fbo.gov/?s=opportunity&mode=form&id=48b393a8498798f078ab8d29612b5e15&tab=core&_cview=0

[12] *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success* (DHS Office of the Inspector General, Feb. 27, 2017), p. 2 https://permanent.access.gpo.gov/gpo78494/OIG-17-40-Feb17.pdf.

The SORN in effect authorizes the creation of secret files. According to the SORN, "[t]he Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and those of the Judicial Redress Act (JRA) if applicable, because it is a law enforcement system."[13] The exemptions include protections pertaining to disclosure, access, relevance, notification, accuracy, and dissemination of information as well as availability of judicial recourse.

According to the SORN, DHS will consider "individual requests to determine whether or not information may be released."[14] But that procedure provides no assurance that records will actually be released. In addition, individuals may well be unable to identify which DHS component would have information or why DHS might have such information. And they may not even know that the information has been collected.

In any event, only citizens and lawful permanent residents are specifically covered by Privacy Act protections, and the Trump administration has eliminated expanded coverage to other non-citizens.[15] If a request is instead made under the Freedom of Information Act (FOIA) for an individual's A-file or other information collected pursuant to the SORN, and incorrect information is identified, FOIA does not provide an avenue for correcting the information.

CONCLUSION

For the reasons stated above, DHS should cease collection of information from social media and the internet, expunge from A-files information already collected, and rescind the SORN.

---

[13] Exemptions Promulgated for the System, https://www.federalregister.gov/documents/2017/09/18/2017-19365/privacy-act-of-1974-system-of-records. Specifically, the system is exempted "from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2): 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (e)(12), (f), (g)(1), and (h). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2): 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f)."

[14] Record Access Procedure, https://www.federalregister.gov/documents/2017/09/18/2017-19365/privacy-act-of-1974-system-of-records

[15] Executive Order: Enhancing Public Safety in the Interior of the United States (Office of the Press Secretary, The White House, Jan. 25, 2017), https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.