



25 Massachusetts Avenue, NW
Suite 335
Washington, DC 20001
202 232 5590
202 464 3590 (fax)
www.irl.org

Board of Directors

Hon. Elizabeth A. Hacker (Ret.)
Hon. Mahlon F. Hanson (Ret.)
Jeffrey R. Parkin
Daniel A. Stein

**Executive Director
& General Counsel**

Dale L. Wilcox¹

Director of Litigation

Christopher J. Hajec²

Senior Counsel

Michael M. Hethmon³

Staff Counsel

Elizabeth A. Hohenstein⁴
Mark S. Venezia⁵

**Director of Investigations
& Staff Counsel**

Julie B. Axelrod⁶

**Director of Legislative Affairs
& Staff Counsel**

Sarah R. Rehberg⁷

Of Counsel

Kris W. Kobach⁸
John M. Miano⁹

*IRLI is a public interest law firm
working to protect the American
people from the negative effects of
uncontrolled immigration.*

*IRLI is a supporting organization
of the Federation for American
Immigration Reform.*

¹Admitted in DC & IN

²Admitted in DC & PA

³Admitted in DC & MD

⁴Admitted in DC & VA

⁵Admitted in DC & VA

⁶Admitted in DC & CA

⁷Admitted in DC & MD

⁸Admitted in NE & KS

⁹Admitted in DC, NJ, & NY

October 16, 2017

Jonathan R. Cantor
Acting Chief Privacy Officer
Privacy Office
245 Murray Lane SW
U.S. Department of Homeland Security
Washington, DC 20528-0655

**DHS Docket Number 2017-0038: Public Comment of the
Immigration Reform Law Institute Regarding Modified Privacy
Act System of Records**

Dear Acting Chief Cantor:

The Immigration Reform Law Institute (“IRLI”) submits the following public comment to the U.S. Department of Homeland Security (“DHS”) in response to the Agency’s Notice of Modified Privacy Act System of Records, as published in the Federal Register on September 18, 2017. *See Privacy Act of 1974; System of Records*, DHS Docket No. 2017-0038, 82 Fed. Reg. 43556-43565.

IRLI is a non-profit public interest law organization that exists to defend the rights of individual Americans and their local communities from the harms and challenges posed by mass migration to the United States, both lawful and unlawful. IRLI works to monitor and hold accountable federal, state, and local government officials who undermine, fail to respect, or fail to comply with our national immigration and citizenship laws. IRLI also provides expert immigration-related legal advice, training, and resources to public officials, the legal community, and the general public.

IRLI supports DHS’s Notice of modifications to the current system of immigration record-keeping entitled, “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.” As stated by DHS in its Federal Register Notice, this system of records, generally referred to as A-Files, “contains information regarding transactions involving an individual as he or she passes through the U.S. immigration process.”

According to recent statements made by a DHS spokesperson, the Agency has been including some of the information outlined in its Notice – and consequently discussed in this Comment – in A-Files for the last several years.¹ The spokesperson claims the Agency is just now publishing its Notice in an effort to be transparent and does not represent new policy.² Regardless of when DHS actually began engaging in the activities described herein, IRLI applauds the Agency’s efforts to update its recordkeeping efforts to protect U.S. national security and ensure immigration authorities are able to act based on complete information.

In particular, this comment will focus on two key modifications as put forth in the Notice: modification Number (5) and modification Number (11).

I. IRLI supports modification Number (5).

Modification Number (5) makes important common-sense updates to the DHS system of immigration record-keeping. Its changes would “expand the categories of records” to include, among other things, “social media handles, aliases, associated identifiable information, and search results...” Compiling these expanded categories of information is critical to creating and maintaining a comprehensive A-File file and is consistent with an overall rational system of record-keeping in-line with U.S. national security interests.

At a time in our country’s history when terrorist attacks are all too frequent, those protecting our nation’s borders must be ever-vigilant in who is allowed to enter our nation and under what conditions. Indeed, the issue of terrorists and terrorist organizations using social media to plan and carry out attacks, as well as seek new recruits, is a real national security threat that has been examined by Congress on numerous occasions.³

One example of such Congressional scrutiny is a Senate Homeland Security and Governmental Affairs Committee hearing held on May 7, 2015. At the hearing, entitled, *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment*, several witnesses testified regarding the

¹ *Federal Plans to Keep Files of Immigrant Social Media Activity Causes Alarm*, NPR, Sept. 30, 2017, <http://www.npr.org/2017/09/30/554557044/federal-plan-to-keep-files-of-immigrant-social-media-activity-causes-alarm>. See also, DHS Directives System, *Privacy Policy for Operational use of Social Media*, Instruction Number 110-01-001, Revision Number 00 (Issued June 8, 2012).

² *Id.*

³ See U.S. Senate Committee on Homeland Security and Governmental Affairs, Majority & Minority Staff Report: “Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat” (May 8, 2008); U.S. House of Representatives’ Committee on Homeland Security: Subcommittee on Counterterrorism and Intelligence Hearing: “Jihadist use of Social Media – How to Prevent Terrorism and Preserve Innovation” (Dec. 6, 2011); U.S. House of Representatives’ Committee on Homeland Security: Subcommittee on Counterterrorism and Intelligence Hearing: “DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy” (Feb. 16, 2012); U.S. House of Representatives’ Committee on Homeland Security Hearing: “Terrorism Gone Viral: The Attack in Garland, Texas and Beyond” (June 3, 2015); U.S. Senate Committee on Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations Hearing: “ISIS Online: Countering Terrorist Radicalization & Recruitment on the Internet & Social Media” (July 6, 2016).

ways in which terrorist organizations, including the Islamic State in Iraq and Syria (ISIS), use social media to encourage and motivate individuals to become followers and carry out attacks in the U.S. and abroad.

J.M. Berger with the Brookings Institution, who testified at the hearing, highlighted the increasing use of social media by terrorists, and in particular, ISIS. Mr. Berger described the three major components of ISIS's social media campaign.⁴ First, to disseminate propaganda to generate support for the group.⁵ Next, to disseminate propaganda designed to manipulate its enemies' perceptions and political reactions.⁶ And finally, to seek new recruits.⁷ Mr. Berger went on to testify that while ISIS "is not the first group to employ social media as a tool for recruitment and propaganda...its innovative and aggressive approach has afforded it an unprecedented level of success, and its activities will likely provide a template for future extremist initiatives." Adding to the urgency of his testimony, Mr. Berger's appearance before the Committee came just two months after the Brookings Institution released a report he co-authored that revealed that in the fall of 2014, there were "no fewer than 46,000 Twitter accounts supporting ISIS."⁸

At the same hearing, Mr. Peter Bergen, Director of the National Security Studies Program at the New America Foundation, similarly attested to the growing use and influence of social media by terrorists. He stated:

More than eight out of ten of the 62 individuals New America identified as involved in Syria-related militancy – with either ISIS or the al-Qaeda-affiliated Nusra Front – were active in **online jihadist circles**. This is something of a boon for law enforcement as **many of these militants are prolific posters on publicly available social media, which it is perfectly legal for the FBI and police departments to monitor**. Militants in the United States today **radicalize after reading and interacting with propaganda online** and have little or no physical interaction with other extremists. **This trend has been going on for the past several years....Social media has dramatically accelerated this trend.**

(emphasis added).⁹ Accordingly, Mr. Bergen's statement underscores the rapidly growing use of social media by violent terrorist organizations who desire to radicalize foreign fighters seeking to

⁴ U.S. Senate, Committee on Homeland Security and Governmental Affairs Hearing: "Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment" (Written Statement of J.M. Berger, Nonresident Fellow, Project on U.S. Relations with the Islamic World, The Brookings Institution) (May 7, 2015).

⁵ *Id.* at p.2.

⁶ *Id.*

⁷ *Id.*

⁸ J.M. Berger and Jonathon Morgan, The Brookings Institution, *The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter* (March 2015).

⁹ U.S. Senate, Committee on Homeland Security and Governmental Affairs Hearing: "Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment" (Written Statement of Peter Bergen, Director, International Security Program, The New America Foundation) (May 7, 2015).

enter the country, while highlighting the organizations' efforts to recruit vulnerable populations within the U.S to carry out their attacks.

Alarminglly, Messrs. Berger and Bergen are only two of many congressional witnesses corroborating such behavior.¹⁰ To therefore handcuff immigration authorities and expect them to not research, review, analyze, collect, maintain or otherwise even consider an individual's social media presence as modification No. 5 entails would thereby create a gaping hole in our immigration screening process and record-keeping system that would put the needs of those trying to do harm over the safety of law-abiding U.S. citizens and residents.

Some opponents of this Notice have argued that collecting and maintaining information posted using social media is an unconstitutional invasion of privacy. However, DHS only captures social media that is posted publicly and therefore not subject to claims of such violations. Indeed, it is well-established that while the Fourth Amendment to the U.S. Constitution protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," these protections only apply when an individual has a "reasonable expectation of privacy."¹¹

In the age of the internet, it is no secret that any information posted publicly by an individual online may be viewed by anyone with an internet connection. It is therefore unreasonable that anyone posting information publicly via social media would believe that such information is private and therefore immune from government detection absent a warrant. It is particularly unreasonable that an individual applying for an immigration benefit – who generally must consent to a background check as part of the application process anyway – to expect his or her postings will be kept private and not be seen, collected, or otherwise used for the benefit of administering authorities.

The same rings true for any aliases an individual may use when publishing such information, including any "associated identifiable information" or "search results" that may yield from such an account. Any expectation of privacy of these categories of publicly posted information is *per se* unreasonable. Just as the government may request a married woman's maiden name in order to conduct a thorough background check on her pre-marriage activities, the ability to use aliases, pseudonyms, and otherwise change one's identity on the internet have similarly necessitated researching and collecting information on online aliases as part of a comprehensive investigation for one's A-File.

Accordingly, IRLI supports modification Number (5) as a common-sense update to our country's immigration record-keeping system.

¹⁰ See Footnote 3.

¹¹ U.S. CONST. amend. IV.; *Katz v. United States*, 389 U.S. 347 (1967).

II. IRLI supports modification Number (11).

Similar to modification Number (5), modification Number (11) makes important common-sense updates to DHS's system of record-keeping. Its changes would:

[U]pdate 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[.]

By proposing such a modification, DHS is merely notifying individuals that it will continue to do what it has been doing for years: including already publicly available information about those seeking an immigration benefit in that individual's immigration record. Whether the collected information is comprised of electronic files from the internet – or paper documents from the local courthouse – it makes no difference. The common thread and key point is that the information being reviewed and stored is “public.”

As such, the “updates” made by DHS in this section do not expand, create, or otherwise alter preexisting authority by the Agency to review that which is already publicly available. The change does not somehow allow DHS to access private Facebook correspondence, learn or maintain internet account passwords, or unseal records that have been made confidential without first going through the proper legal channels. Consequently, even the most well-intentioned allegations of privacy violations are unfounded.

Accordingly, IRLI supports modification Number (11) as a common-sense update to our country's immigration record-keeping system.

III. Conclusion.

In conclusion, IRLI supports DHS's modifications to the current system of immigration records per the Agency's “Notice of Modified Privacy Act System of Records” as published in the Federal Register on September 18, 2017. In particular, IRLI supports modifications Numbers (5) and (11), as common-sense updates to the nation's A-File recording-keeping system to ensure a comprehensive system of immigration records is in place to assist in facilitating the Agency's mission of protecting our national security.

Respectfully submitted,



Sarah R. Rehberg

Director of Legislative Affairs & Staff Counsel

IRLI