epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER to

DEPARTMENT OF STATE

Proposed Information Collections: Application for Nonimmigrant Visa; Electronic Application for Immigrant Visa and Alien Registration

83 FR 43952 and 43951

September 27, 2018

By notices published August 28, 2018, the U.S. Department of State proposes an intrusive information collection system for immigrant and nonimmigrant visa applications.[1] The State Department proposes to ask visa applicants to disclose all social media identifiers, phone numbers, and email addresses used within the past five years. The State Department intends to obtain access to the private social media activities and personal communications of visa applicants.

The State Department stated that it plans to use the personal data collected for "identity resolution and vetting purposes" to determine visa eligibility.[2] The agency has not provided further details about other uses of social media identifiers and personal communications nor has it made clear how such data will be protected, since data of non-US persons is typically not subject to

[1] *30-Day Notice of Proposed Information Collection: Electronic Application for Immigrant Visa and Alien Registration*, 83 FR 43952 (Aug. 28, 2018) (hereafter Immigrant Visa Notice), *available at*: https://www.gpo.gov/fdsys/pkg/FR-2018-08-28/pdf/2018-18595.pdf; *30-Day Notice of Proposed Information Collection: Electronic Application for Nonimmigrant Visa*, 83 FR 43951 (Aug. 28, 2018)(hereafter Nonimmigrant Visa Notice), *available at*: https://www.gpo.gov/fdsys/pkg/FR-2018-08-28/pdf/2018-18594.pdf (hereafter, "Notices").

[2] *Id.*

protection under the Privacy Act of 1974, which otherwise safeguards the data collected by federal agencies.[3]

Pursuant to the agency's request for comments, the Electronic Privacy Information Center ("EPIC") submits these comments to request that the Department: (1) retract the proposal to collect social media identifiers and personal communications information; and (2) review the appropriateness of using social media and personal communications information to make visa determinations.

I. Introduction

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and protect privacy, the First Amendment, and constitutional values.[4] EPIC has a particular interest in preserving the right of people to engage in First Amendment protected activities without the threat of government surveillance. EPIC has repeatedly urged federal agencies not to use social media to make adverse determinations about individuals.[5] EPIC has also advocated for better privacy protections for telecommunications metadata and sought transparency where the government seeks to collect telecommunications data.[6]

---

[3] 5 U.S.C. 552a(a)(2)("the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence.")

[4] EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.

[5] Comments of EPIC, *Supplemental Questions for Visa Applicants*, Oct. 2, 2017, https://epic.org/apa/comments/EPIC-DOS-Visas-SocialMediaID-2017.pdf; Comments of EPIC, *Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants*, May 18, 2017, https://epic.org/apa/comments/EPIC-DOS-Social-Media-ID-Collection-Comments.pdf; Comments of EPIC, *Agency Information Collection Activities: Electronic Visa Update System,* May 30, 2017, https://epic.org/apa/comments/EPIC-CBP-Social-Media-ID-Collection-Comments.pdf; Comments of EPIC, *Agency Information Collection Activities: Arrival and Departure Record (Forms I-94 and I-94W), and Electronic System for Travel Authorization,* Sep. 30, 2016, https://epic.org/apa/comments/EPIC-Comments-DHS-Social-Media-ID- Collection.pdf; Comments of EPIC, *Privacy Act of 1974; Department of Homeland Security/ALL—038 Insider Threat Program,* Mar. 28, 2016, https://epic.org/apa/comments/EPIC-DHS-Insider-Threat-Comments.pdf.

[6] *See, e.g.*, Letter from EPIC to the House Comm. on the Judiciary: Subcomm. on Crime, Terrorism, Homeland Security, and Investigations (Apr. 4, 2017), https://epic.org/testimony/congress/EPIC-HJC-DEA-Apr2017.pdf; EPIC *et al.*, *Petition to Repeal C.F.R. § 42.6 ("Retention of Telephone Toll Records* (Aug. 4, 2015),

EPIC has previously sued the Department of Homeland Security ("DHS") to obtain documents related to a DHS social network and media monitoring program.[7] These documents revealed that the agency had paid over $11 million to an outside company, General Dynamics, to engage in monitoring of social networks and media organizations and to prepare summary reports for DHS.[8] According to the documents obtained by EPIC, General Dynamics would "monitor public social communications on the Internet," including the public comments sections of NYT, LA Times, Huffington Post, Drudge, Wired's tech blogs, and ABC News.[9] DHS also requested monitoring of Wikipedia pages for changes[10] and announced its plans to set up social network profiles to monitor social network users.[11]

DHS required General Dynamics to monitor not just "potential threats and hazards" and "events with operational value," but also paid the company to "identify[] media reports that reflect adversely on the U.S. Government [or] DHS . . . ."[12] The DHS clearly intended to "capture public reaction to major government proposals."[13] DHS instructed the media monitoring company to generate summaries of media "reports on DHS, Components, and other Federal Agencies: positive and negative reports on FEMA, CIA, DOS, ICE, etc. as well as organizations outside the DHS."[14]

---

https://epic.org/privacy/fcc-data-retention-petition.pdf; EPIC FOIA Request and Request for Expedited Processing – Surveillance of Reporters (May 14, 2013) (seeking the legal basis for the government access to telephone, text message, and email communications of reporters), https://epic.org/foia/doj/epic-olc-reporter-surveillance-foia-request.pdf.

[7] EPIC, *EPIC v. Department of Homeland Security: Media Monitoring*, https://epic.org/foia/epic-v-dhs-media-monitoring/.

[8] DHS Social Media Monitoring Documents, *available at* https://epic.org/foia/epic-v-dhs-media-monitoring/EPIC-FOIA-DHS-Media-Monitoring-12-2012.pdf; *See also* Charlie Savage, *Federal Contractor Monitored Social Network Sites*, New York Times, Jan. 13, 2012, http://www.nytimes.com/2012/01/14/us/federal-security-program- monitored-public-opinion.html.

[9] DHS Social Media Monitoring Documents at 127, 135, 148, 193.

[10] *Id.* at 124, 191.

[11] *Id.* at 128

[12] *Id.* at 51, 195

[13] *Id.* at 116.

[14] *Id.* at 183, 198.

The documents obtained by EPIC through its Freedom of Information Act lawsuit led to a Congressional hearing on DHS social network and media monitoring program.[15] EPIC submitted a statement for the record for that hearing opposing the agency's media monitoring and called for the immediate end of the program.[16] Members of Congress expressed concern about the federal agency's plan to monitor social media.[17]

Given government misuse of social media monitoring techniques in the past, EPIC is skeptical of the State Department's proposal to use social media to scrutinize visa applicants during the vetting process. EPIC opposes this proposal.

II. The Lack of Transparency Surrounding the Department's Proposal Increases the Prospect of Abuse, Mission Creep, and Disproportionate Risks for Marginalized Groups

It is not clear how the DOS intends to use the social media identifiers or phone numbers and email addresses. While DOS proposes to request social media identifiers, phone numbers, and email addresses used within the past five years of the application's filing date, DOS has neither provided additional limitations on collection nor explained how this information will help determine visa eligibility. With regard to social media identifiers, for example, DOS indicates that the social media platforms listed on applicant questionnaires "may be updated by the Department by adding or removing platforms,"[18] without describing criteria for adding or removing social

[15] *See DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy: Hearing Before the Subcomm. on Counterterrorism and Intelligence of the H. Comm. on Homeland Security*, 112th Cong. (2012).
[16] Marc Rotenberg, President and Ginger McCall, EPIC Open Government Project Director, *Statement for the Record for Hearing on DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy* (Feb. 16, 2012), https://epic.org/privacy/socialmedia/EPIC-Stmnt-DHS-Monitoring-FINAL.pdf.
[17] Andrea Stone, *DHS Monitoring of Social Media Under Scrutiny by Lawmakers,* Huffington Post (Feb. 16, 2012), http://www.huffingtonpost.com/2012/02/16/dhs-monitoring-of-social-media_n_1282494.html; *Congress Grills Department of Homeland Security,* EPIC, Feb. 16, 2012, https://epic.org/2012/02/congress-grills-department-of-.html.
[18] Nonimmigrant Visa Notice.

media platforms that DOS finds relevant. Likewise, DOS provides no description of how email address and phone number information will be used.

Other federal agencies have a history of using social media for controversial purposes. For example, DHS has monitored social and other media for dissent and criticism of the agency[19] and for signs of potential terrorist activity among immigrants and naturalized citizens.[20] Federal agencies have a similar history of monitoring emails and phone records for controversial purposes. Section 702 of the Foreign Intelligence Surveillance Act was reauthorized in January 2018, allowing the DOJ to search and read emails from millions of Americans and foreigners, as the government had for years prior to the 2013 Edward Snowden disclosures. In 2017, the NSA tripled its collection of U.S. phone call and text message records for national security surveillance, monitoring at least 534 million records of numbers and frequencies of calls and texts.[21] Will the DOS monitor for similar speech that is critical of U.S. policy, or monitor for emails and phone calls to persons who are critical of U.S. policy? Will mere dissent or association with dissenters constitute grounds for denying entry into the U.S.? Additionally, will alien visitors who provide their social media identifiers open up their social network associations to scrutiny? How long will social media identifiers and personal communications information be retained and who will they be shared with? How will the DOS prevent Muslim and Arab Americans from being scrutinized more harshly?

---

[19] Marc Rotenberg, President and Ginger McCall, EPIC Open Government Project Director, *Statement for the Record for Hearing on DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy*, 1-3, Feb. 16, 2012, https://epic.org/privacy/socialmedia/EPIC-Stmnt-DHS-Monitoring-FINAL.pdf.

[20] In a Federal Register notice from last year, DHS indicated that the agency has been collecting social media and associated identifiable information to monitor lawful permanent residents and naturalized citizens. *Notice of Modified Privacy Act System of Records,* 82 FR 43556 (Sept. 18, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-09-18/pdf/2017-19365.pdf.

[21] *Dustin Volz, Spy Agency NSA Triples Collection of Phone Records: Official Report*, Reuters (May 4, 2018), https://www.reuters.com/article/us-usa-cyber-surveillance/spy-agency-nsa-triples-collection-of-u-s-phone-records-official-report-idUSKBN1I52FR.

Answers to these questions should be provided prior to adoption of the Department's proposal to acquire the social media identifiers of people suspected of no crime.

This proposal leaves the door open for abuse, mission creep, and the disproportionate targeting of Muslim and Arab Americans among other groups. This proposal is especially alarming in light of past misuses of social media and communications information from all levels of government[22] as well as the Trump administration's controversial travel ban.[23] The State Department has provided no details of how the agency will tailor the use of social media identifiers and communications information to ensure their use does not expand beyond the stated purpose or prevent the targeting of individuals merely engaged in First Amendment protected activities.

III. Indiscriminate Scrutiny of Social Media Accounts and Personal Communications Information Chills First Amendment Protected Activities

Social Media Accounts

DOS's proposal to collect social media identifiers of visa applicants also implicates the First Amendment and will have a chilling effect on protected speech. Freedom of speech and expression are core civil liberties and have been strongly protected by the Constitution and the

[22] Elizabeth Dwoskin, *Police Are Spending Millions of Dollars to Monitor the Social Media of Protesters and Suspects,* Washington Post (Nov. 18, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/11/18/police-are-spending-millions-to-monitor-the-social-media-of-protesters-and-suspects/; *Map: Social Media Monitoring By Police Departments, Cities, and Counties,* Brennan Center for Justice, Nov. 16, 2016, https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties; Eric Yoder, *Beware What You Post: Federal Employees May Face Government Scrutiny on Social Media,* Washington Post (May 12, 2016), https://www.washingtonpost.com/news/powerpost/wp/2016/05/12/beware-what-you-post-federal-employees-may-face-government-snooping-on-social-media/; Evan Halper, U.S. *Government's Embattled Email Surveillance Program Proves Resilient*, Los Angeles Times (Dec. 13, 2017), http://www.latimes.com/politics/la-na-pol-government-surveillance-emails-20171213-story.html (noting "For example, if an American participates in or promotes an event abroad as benign as a climate change protest or an academic conference on international affairs, they could get swept into the surveillance, according to [Section 702] interpretations.")

[23] Alex Emmons, *Activists Worry That Social Media Vetting of Visa Applicants Could Quietly Expand Trump's Muslim Ban,* The Intercept (Mar. 23, 2017), https://theintercept.com/2017/03/23/activists-worry-that-social-media-vetting-of-visa-applicants-could-quietly-expand-trumps-muslim-ban/.

U.S. courts.[24] These rights extend to non-U.S. citizens.[25]

Many people around the world use social media, including Facebook and Twitter, to support democratic movements and to campaign for political reform.[26] But these political views reflect the specific circumstances of national political systems and regional political conflict, and there is some risk that comments taken out of context could discourage political reform efforts. For example, social media is credited with empowering the Arab Spring and allowing Egyptians to remove former President Hosni Mubarak from power.[27] Social media also played a pivotal role in the 2013 Gezi Park protests in Turkey, the recent anti-Putin protests in Russia, which were sparked by a blog post and YouTube video,[28] and the proliferation of activist movements like Black Lives

[24] *See, e.g.*, *Minnesota Voters Alliance v. Mansky*, 138 S. Ct. 1876 (2018) (holding that a state ban on wearing 'a political badge, political button, or other political insignia "plainly restricts'"…First Amendment freedom of speech); *United States v. Stevens*, 130 S. Ct. 1577, 1585 (2010) (holding that the "First Amendment itself reflects a judgment by the American people that the benefits of its restrictions on the Government outweigh the costs"); *see also NAACP v. Alabama ex. rel. Patterson,* 357 U.S. 449 (1958) (holding that immunity from state scrutiny of membership lists was related to the right of freedom of association and fell under the 14th Amendment of the U.S. Constitution); *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015) (holding that a city ordinance that required hotels to make their registries available to the police on demand was unconstitutional under the 4th Amendment of the U.S. Constitution).

[25] *See* David Cole, *Are Foreign Nationals Entitled to the Same Constitutional Rights as Citizens?,* 25 T. Jefferson L. Rev. 367-388 (2003) ("foreign nationals are generally entitled to the equal protection of the laws, to political freedoms of speech and association, and to due process requirements of fair procedure where their lives, liberty, or property are at stake.").

[26] The Associated Press, *Social Media is the New Heart of Political Protests*, WTOP News (June 22, 2018), https://wtop.com/social-media/2018/06/todays-protests-many-voices-social-media-not-1-leader/; Sophie Hutchinson, *Social media Plays Major Role In Turkey Protests,* BBC (Jun. 4, 2013), http://www.bbc.com/news/world-europe-22772352; David Auerbach, *The Bernie Bubble,* Slate (Feb. 17, 2016), http://www.slate.com/articles/technology/future_tense/2016/02/the_bernie_sanders_campaign_owes_a_lot_to_social_media.html.

[27] Amitava Kumar, *'Revolution 2.0': How Social Media Toppled A Dictator,* NPR (Feb. 8, 2012), http://www.npr.org/2012/02/08/145470844/revolution-2-0-how-social-media-toppled-a-dictator; Ramesh Srinivasan, *Taking Power Through Technology in the Arab Spring,* Al Jazeera (Oct. 26, 2012), http://www.aljazeera.com/indepth/opinion/2012/09/2012919115344299848.html.

[28] Steve Dorsey, *Turkey's Social Media And Smartphones Key To 'Occupy Gezi' Protests,* Huffington Post (Jun. 10, 2013), http://www.huffingtonpost.com/2013/06/09/turkey-social-media-smartphones-occupy-gezi-protests_n_3411542.html; Julia Ioffee, *What Russia's Latest Protests Mean for Putin,* The Atlantic (Mar. 27, 2017), https://www.theatlantic.com/international/archive/2017/03/navalny-protests-russia-putin/520878/.

Matter[29] and #MeToo.[30]

DOS suggests that social media identifiers will be used for vetting purposes.[31] However, the proposal assumes that social media provides an accurate picture of a person and those they are close with. People connect with others on social media for many reasons. An individual's "friend" on a social media site could range from a close friend to an acquaintance to someone they may never have met. Often individuals connect to people on social media who have completely different perspectives and world views. Furthermore, the proposal fails to identify the parameters of using social media as a vetting mechanism. Neither notice describes, for example, the extent that possible connections will be used in the vetting process and whether the social media accounts of U.S. citizens may be used as part of the vetting process.

The proposal also fails to explain how DOS will actually use social media as part of the vetting process. Many individuals have been on social media for years and have created a permanent record of their lives.[32] Teenagers are routinely warned to be careful of what they post on social media,[33] however teenagers and adults have made posts on social media which they later regret and may not be an actual reflection of who they are.[34] This should be taken into account when using social media to vet those entering the country. Social media does not necessarily reflect who a person truly is and taking posts out of context has the potential to wrongly deny

---

[29] Caroline Simon, *How Social Media Has Shaped Black Lives Matter, Five Years Later*, USA Today (Jul. 28, 2018), https://www.usatoday.com/story/news/2018/07/12/black-lives-matter-movement-and-social-media-after-five-years/778779002/.

[30] Sandee LaMotte, *How #MeToo Could Move From a Social Campaign to Social Change*, CNN News (Nov. 9, 2017), https://www.cnn.com/2017/10/30/health/metoo-legacy/index.html (noting how the 10-year old MeToo movement already showed promise of transforming from a campaign into a social change after two weeks on social media).

[31] Nonimmigrant Visa Notice.

[32] Alexandra Mateescu et. al., *Social Media Surveillance and Law Enforcement*, DATA & CIVIL RIGHTS (Oct. 27, 2015), http://www.datacivilrights.org/pubs/2015-1027/Social_Media_Surveillance_and_Law_Enforcement.pdf.

[33] Franki Rosenthal, *Caution ahead: The dangers of social media*, SUN SENTINEL (Feb. 2, 2016), http://www.sun-sentinel.com/teenlink/college/tl-caution-ahead-the-dangers-of-social-media-20160202-story.html.

[34] Alyssa Giacobbe, *6 ways social media can ruin your life*, BOSTON GLOBE (May 21, 2014), https://www.bostonglobe.com/magazine/2014/05/21/ways-social-media-can-ruin-your-life/St8vHIdqCLk7eRsvME3k5K/story.html.

people entry because of an inside joke or posturing that DOS does not understand from viewing certain information in isolation.[35] Furthermore, the proposal runs the risk of making what is not on social media seem suspect. Some individuals may not be active on social media or may not have any social media accounts at all and the Department has failed to say what impact, if any, this may have on the vetting process.

According to recent reporting, DHS has made its social media data "searchable by tone" to conduct emotional analysis on visa applicants.[36] It is not clear whether DOS intends to use similar analysis methods. Use of such artificial intelligence tools raises many problems. It is difficult for algorithms to understand the complexity of language—sarcasm and slang are very difficult to detect.[37] The shortcomings of natural language processing could distort the results of an algorithm meant to classify statements by tone.

Furthermore, the lack of algorithmic transparency amplifies these problems. If these algorithms are used to make decisions about someone's ability to enter the U.S., they should not be secret. Without algorithmic transparency, algorithms used to profile people are prone to errors and abuse. Many of the problems caused by algorithms used in the criminal justice system are present in the immigration context as well. Law enforcement officials often use algorithms to determine the guilt of a criminal defendant, while denying the defendant access to the source code that

---

[35] Mateescu et. al., *Social Media Surveillance*; Brandon Giggs, *Teen failed for Facebook 'joke' is released*, CNN (Jul. 13, 2013) (discussing a teenager who was arrested after making a "threat" that, when viewed in context, appears to be sarcasm), http://www.cnn.com/2013/07/12/tech/social-media/facebook-jailed-teen/; Ellie Kaufman, *Social Media Surveillance Could have a Devastating Impact on Free Speech. Here's Why.*, MIC (Jan. 19, 2016), https://mic.com/articles/132756/social-media-surveillance-could-have-a-devastating-impact-on-free-speech-here-s-why.

[36] Aaron Cantú and George Joseph, *Trump's Border Security May Search Your Social Media by 'Tone,'* The Nation (Aug. 23, 2017), https://www.thenation.com/article/trumps-border-security-may-search-your-social-media-by-tone/.

[37] *Id.*; Ben Conarck, *Sheriff's Office's Social Media Tool Regularly Yielded False Alarms,* The Florida Times-Union (May 30, 2017), http://jacksonville.com/news/public-safety/metro/2017-05-30/sheriff-s-office-s-social-media-tool-regularly-yielded-false.

produced those results.[38] Similarly, an algorithm could determine whether immigrants are denied visas. Without access to the source code, it is impossible to identify errors in the analysis or determine why an individual was denied a visa. If DOS intends to delegate its decision-making to computers they must disclose the code that led to their decisions.

Government programs that threaten important First Amendment rights are immediately suspect and should only be undertaken where the government can demonstrate a compelling interest that cannot be satisfied in another way.[39] Government programs that scrutinize online comments, dissent, and criticism for the purpose of vetting visitors prior to entry into the U.S. send a chilling message to all users of social media—which increasingly provides important forums to share ideas, engage in debates, and explore new ideas.

Concern over the how the government uses social media is widespread and several questions remain unanswered. Earlier this year, several members of the House of Representatives sent a letter to Attorney General Jeff Sessions raising concerns about how the federal government and federal law enforcement agencies used technologies that monitored social media.[40] Those Representatives noted how social media was effectively being used to monitor people who were suspected of no wrongdoing in violation of their Fourth Amendment rights stating:

> There is evidence that social media data has been used to monitor protests and activists…An investigator at the Oregon Department of Justice used a service called DigitalStakeout to search Twitter for tweets using the hashtag #BlackLivesMatter. On the basis of his tweets – which included political cartoons and commentary but no indications of criminal activity or violence – the Department's own Director of Civil Rights was deemed a "threat to public safety.[41]

[38] EPIC, *Algorithms in the Criminal Justice System*, https://epic.org/algorithmic-transparency/crim-justice/.
[39] *See, e.g.*, *NAACP v. Button*, 83 S. Ct. 328 (1963); *Citizens United v. Fed. Election Comm'n*, 130 S. Ct. 876 (2010).
[40] Letter to Jeff Sessions from Keith Ellison et al., May 2, 2017, https://www.documentcloud.org/documents/3696481-House-Democrats-Letter-to-Sessions-re-Social.html.
[41] *Id.*

The same concerns are present in DOS's current proposal and these concerns must be addressed before any further steps are taken.

Phone numbers and email addresses

DOS's proposal to collect all phone numbers and email addresses used within five years of the application filing date will also have a chilling effect on protected speech, as previously discussed. The collection implicates First Amendment freedom of association as well.

Along with social media, cell phones (especially smartphones and androids) and email accounts are the most popular ways of sending and receiving information.[42] Even in poor countries, approximately 89.4% of people use cell phones for daily communication.[43] Many people also place calls and send text messages from more than one telephone number,[44] and many hold multiple email accounts.[45] By the end of 2019, over 246 billion emails are expected to be sent every day, used by at least one-third of the world's population.[46]

DOS's proposal is problematic because it does not mention how telephone number and email addresses will be used for vetting purposes, nor the extent that DOS will examine the call records and email metadata. Under the reauthorization of FISA Section 702, the government can already collect called or texted numbers, the time a call or text was made, and the duration of the call. Access to a wealth of phone records can also be obtained through a program known as "Hemisphere" run by the telecommunications company AT&T. According to reporting, AT&T has

---

[42] Larry Alton, *Phone Calls, Texts, or Email? Here's How Millenials Prefer to Communicate*, Forbes (May 11, 2017), https://www.forbes.com/sites/larryalton/2017/05/11/how-do-millennials-prefer-to-communicate/#2f2675866d6f.
[43] Tim Fernholz, *More People Around the World Have Cell Phones Than Land-Lines*, Quartz (Feb. 25, 2014), https://qz.com/179897/more-people-around-the-world-have-cell-phones-than-ever-had-land-lines/.
[44] Zachary Davies Boren, *There Are Officially More Mobile Devices Than People In the World*, Independent (Oct. 7, 2014), https://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html.
[45] *Email Statistics Report, 2015-2019*, The Radicati Group (March 2015), 3, *available at*: http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf.
[46] *Id.* (noting that in 2015, over 205 billion emails was sent every day).

been collecting call records for decades and providing access to government authorities, particularly the Drug Enforcement Agency ("DEA").[47] Documents recently obtained by EPIC from a Freedom of Information Act lawsuit revealed that access to Hemisphere records extended beyond the DEA and included the Federal Bureau of Investigation and Customs and Border Protection.[48] Will DOS use the phone numbers and email addresses provided to collect metadata for analysis?

Telephone and email metadata can reveal sensitive information. In a study conducted by Stanford researchers, the sensitivity of the telephone metadata of several hundred volunteers was analyzed.[49] From the call records, the researchers were able to infer religious affiliation, medical conditions, and political views among other sensitive and private information.[50] Will DOS analyze phone records and email metadata for evidence of political dissidence to be used in visa application determinations? Will disfavored associations uncovered by telephone records and email metadata be disqualifying? These questions and more must be answered before proceeding with the collection.

Furthermore, it is unclear that searching phone records or emails can be a fair tool to evaluate visa applications. The proposed collection assumes that all texts, calls, and emails were intentionally sent and received. This assumption, however, is easily misleading. For example, what if an applicant's email account was hacked to send messages to people who happen to be criminals, terrorists, or on a government watchlist? Similarly, the proposed collection also does not account for the potential of illegal robocalls. For example, while records of a short phone call from

---

[47] Kenneth Lipp, *AT&T is Spying on Americans for Profit*, DailyBeast (Oct. 25, 2016), https://www.thedailybeast.com/atandt-is-spying-on-americans-for-profit.
[48] EPIC, *EPIC FOIA Docs Show FBI and CBP Accessed "Hemisphere" Records*, https://epic.org/2018/09/epic-foia-docs-show-fbi-and-cb.html.
[49] *See* Jonathan Mayer & Patrick Mutchler, MetaPhone: The Sensitivity of Telephone Metadata (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone- metadata/.
[50] *Id.*

a suspicious number might be read as evidence of nefarious activity with an attempt to avoid traceability, the same call could easily have been an illegal robocall from a spoofed number, which the user unwittingly listened to before hanging up.[51]

All of these concerns regarding the proposed use of social media identifiers, phone numbers, and email accounts must be addressed before implementing this proposal.

IV. The Demand for an Individual's Social Media Identifier and Personal Communications Information Raises Particular Privacy Concerns

The request for "social media identifiers," phone numbers, and email addresses raises a related concern – these particular types of personal information tie together discrete bits of personal data.[52] In the past, the United States has sought to regulate the collection and use of the Social Security Number precisely because of the concern that this leads to government profiling.[53] The availability of the SSN has been shown to contribute to identity theft and financial fraud.[54]

A social media identifier, email account, or phone number is not private in the sense that they are secret. But government collection of this information does raise privacy concerns because it enables enhanced profiling and tracking of individuals. Furthermore, an individual has no way of knowing who in the government may be tracking them and for how long that surveillance could continue. What is initially presented as a way to vet visa applicants can turn into unwarranted, large scale surveillance of innocent people. Immigration and Customs Enforcement Director Tom Homan has indicated that he wants to implement "continuous vetting" after an applicant's visa has

---

[51] Comments of EPIC, *Refreshed Record on Advanced Methods to Target Unlawful Robocalls*, Federal Communications Commission, Sept. 24, 2018, https://epic.org/apa/comments/EPIC-FCC-Robocalls-Refresh-Sept2018.pdf.

[52] *Social Security Numbers*, EPIC, https://epic.org/privacy/ssn/.

[53] Testimony of Marc Rotenberg, Computer Professionals for Social Responsibility, "Use of Social Security Number as a National Identifier," Before the Subcomm. on Social Security of the House Comm. on Ways and Means, 102d Cong., 1st Sess. 71 (February 27, 1991). republished Marc Rotenberg, "The Use of the Social Security Number as a National Identifier," *Computers & Society,* vol. 22, nos. 2, 3, 4 (October 1991); Privacy Act of 1974, 5 U.S.C. §552a (2016).

[54] *Identity Theft*, EPIC, https://epic.org/privacy/idtheft/; *Social Security Numbers*, EPIC, https://epic.org/privacy/ssn.

been granted.[55] This underscores the concern that DOS and other agencies will utilize social media information, emails, and phone records to perpetually monitor immigrants, not just to make visa and other immigration determinations. Neither Notice specifies whether DOS intends to do this, nor whether DOS will preserve an individual's records of this information after the vetting process is complete.

For these reasons we urge the agency to withdraw its proposal to collect and use social media identifiers, phone numbers, and email addresses to make visa determinations.

V. Conclusion

EPIC recommends that DOS retract the proposal to collect social media identifiers, phone numbers, and email addresses. The problems with collecting this information and scrutinizing social media accounts, emails, and phone records of persons not suspected of any wrongdoing are significant and far-reaching. DOS has provided little transparency in how the agency plans to use this information collected or how it will be safeguarded. The proposal undermines privacy and is contrary to First Amendment rights of speech, expression, and association.

Respectfully submitted,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President and Executive Director

/s/ *Jeramie D. Scott*
Jeramie D. Scott
EPIC National Security Counsel

/s/ *Spencer K. Beall*
Spencer K. Beall
EPIC Administrative Law Fellow

[55] Tal Kopan, *Vetting of Social Media, Phones Possible as Part of Travel Ban Review,* CNN (Sept. 12, 2017), http://www.cnn.com/2017/09/12/politics/travel-ban-next-steps/index.html.