10 March 2017

The Honorable John F. Kelly
Secretary of Homeland Security
Department of Homeland Security
301 7th Street SW
Washington, DC 20528

Dear Secretary Kelly,

We, the undersigned coalition of human rights and civil liberties organizations and trade associations write in response to your statement at the House Homeland Security Committee hearing on February 7, 2017, that the Department of Homeland Security would consider requiring visa applicants to provide log-in information (passwords or other credentials) for their social media accounts. We urge you to reject any proposal to require anyone to provide log-in information to their online accounts as a condition of entry into the United States. Demanding log-in information is a direct assault on fundamental rights and would weaken, rather than promote, national security.

Moreover, we are concerned about the numerous reports that Customs and Border Protection officials are demanding access to digital devices and social media information from refugees, visa holders,[1] lawful permanent residents (green card holders), and US citizens.[2] These reports indicate that CBP officials are interrogating travelers about their religious and political views and scrutinizing their reading and viewing habits, news sources, and private communications.

This intensive examination of travelers' digital lives jeopardizes the security of the United States and its citizens and others abroad. It is deeply invasive, burdens fundamental freedoms, has a discriminatory impact, and is not likely to yield useful information.

Invasive review of online activity for travelers jeopardizes security.
CBP's actions may dramatically increase security risks to US citizens, who will likely face similar demands for access to their devices, online accounts, and passwords at foreign borders. Individuals who handle sensitive governmental or corporate information and travel to other countries, whether for business or pleasure, could be compelled to provide access to the

[1] The Committee to Protect Journalists, for example, has documented the scrutiny faced by a number of foreign journalists arriving to the US, including visa holders and lawful permanent residents. *See* Committee to Protect Journalists, "BBC journalist questioned by US border agents, devices searched," Feb. 1, 2017, https://www.cpj.org/2017/02/bbc-journalist-questioned-by-us-border-agents-devi.php.

[2] NASA employee and US citizen Sidd Bikkannavar was detained in Los Angeles until he agreed to give CBP officials access to his US government-issued phone. Loren Grush, The Verge, "A US-born NASA scientist was detained at the border until he unlocked his phone," Feb. 12, 2017, http://www.theverge.com/2017/2/12/14583124/nasa-sidd-bikkannavar-detained-cbp-phone-search-trump-travel-ban.

accounts housing that information; indeed it is a small jump from requiring passwords to social media accounts to requiring passwords for email, financial, e-commerce, or other online accounts, which would unlock troves of personal information. A world where every traveler may have to hand the keys to their online identities over to a government actor is less safe for everyone.

Compromised credentials for social media accounts create enormous security risks for individuals. Many people use their social media accounts to log in to other services; a personal finance service, for example, may offer users the ability to log in with their Facebook or Google account.[3] Maintaining the fidelity of these accounts is a fundamental security concern for many who otherwise may not be comfortable using online services. The creation of a database containing millions of passwords and social media identifiers will also create a significant risk for data breach, as it would undoubtedly be a major target for identity thieves and other bad actors.[4] To mitigate that threat, affected individuals would need to immediately change their passwords, mooting any alleged effectiveness of DHS's plan.

This review is likely to produce a massive amount of information with little utility. Monitoring online activity in social media accounts is questionable as either an efficient or useful way of gathering specific, actionable evidence in support of CBP officials' authority to enforce the immigration and customs laws. Bad actors will find ways to conceal their activity, while most travelers and US citizens caught up in CBP's dragnet will have generated massive amounts of information completely irrelevant to border security, making it more difficult to identify those with malevolent intent.

Moreover, online communications are often extremely dependent on context, making them prone to misinterpretation, especially if officials lack relevant linguistic and cultural background. Scrutinizing travelers' online activity will consume significant amounts of time and personnel resources while yielding little insight.

Demands to access private information intrude upon confidential professional relationships. Anyone with an obligation of confidentiality, whether they be an attorney, a journalist, a member of the clergy, a doctor, or a business executive, will be placed in the

[3] *E.g.* Venmo payments application, https://venmo.com/; Pocket Expense personal finance assistant, https://itunes.apple.com/us/app/pocket-expense-personal-finance-assistant/id424575621.

[4] The Office of Personnel Management, for example, experienced a high-profile breach that exposed more than 22 million individuals' personal information. Patricia Zengerle and Megan Cassella, Reuters, "Millions more Americans hit by government personnel data hack," July 9, 2015, http://www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709. Recent guidance from the Office of Management and Budget to federal agencies regarding data breach notes that passwords are among "[c]ertain data elements [that] are particularly sensitive and may alone present an increased risk of harm to the individual. Shaun Donovan, Director, Office of Management and Budget, "Preparing for and Responding to a Breach of Personally Identifiable Information", Jan. 3, 2017, https://obamawhitehouse.archives.gov/sites/default/files/omb/ memoranda/2017/m-17-12_0.pdf.

untenable position of deciding whether to breach the trust that their clients, patients, and associates have placed in them or stop traveling to the US.[5] Indeed, these professionals may be unable to continue working with or representing US citizens if they cannot travel to the United States without having to reveal confidential information. Foreign scientists, researchers, and experts likewise may be chilled from traveling to the US and working with US colleagues, putting US citizens at a disadvantage and hampering their ability to work in the professions of their choice.

Extensive inquiry into individuals' online activity is profoundly invasive of their privacy and chills freedom of expression, religion, and association. Reports indicate that CBP officials are obtaining travelers' devices and then examining their public and private social media activity, their web browsing history, their contact lists, and the media they have viewed.[6] Even without demanding a person's log-in information, accessing their accounts through an unlocked phone or other device exposes their private thoughts, communications, and relationships.[7] This data may reveal sensitive information that should not be considered fair game for routine, suspicionless scrutiny by the government, including information about their health, sexual orientation, finances, political views, religious beliefs, and reading and purchase history.

Travelers will face a strong incentive to leave their devices at home or delete their accounts entirely, making a trip to the US like traveling back in time. Fears of compelled access by border officials will also discourage travelers to the US from participating on social media, freely reading the news or visiting websites, and communicating with loved ones. These could encourage travelers to curate their online activity before arrival in the US while also impeding their ability to plan legitimate travel. Travelers who do not have smartphones or social media accounts may fear being viewed with suspicion and denied entry due to their inability to turn over any information.

Invasive inquiry into social media activity will likely have a disparate impact on Muslims, including US citizens. Since the Executive Order "Protecting the Nation from Foreign Terrorist Entry Into the United States," people traveling from Muslim-majority countries are being targeted

---

[5] *See* Alexander Ellerbeck, "Security risk for sources as U.S. border agents stop and search journalists", Dec. 9, 2016, https://cpj.org/blog/2016/12/security-risk-for-sources-as-us-border-agents-stop.php.

[6] One Canadian citizen, Fadwa Aloui, was turned away by border agents who reportedly said, "You're not allowed to go to the United States because we found videos on your phone that are against us." Aloui had Arabic-language videos of daily prayers on her phone. Steve Rukavina, CBC News, "Canadian woman turned away from U.S. border after questions about religion, Trump," Feb. 8, 2017, http://www.cbc.ca/news/canada/montreal/canadian-woman-turned-away-from-u-s-border-after-questions-about-religion-trump-1.3972019.

[7] Haisam Elsharkawi, a US citizen, was detained in Los Angeles and "pressured […] to unlock his cellphone so that [CBP officials] could scroll through his contacts, photos, apps and social media accounts." Daniel Vector, New York Times, "What are your rights if a border agent wants to search your phone?" Feb. 14, 2017, https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html.

with the heaviest scrutiny under various "extreme vetting" procedures, including countries not referred to in the Executive Order.[8] Muslim-Americans have even been detained at the border and interrogated about their religious beliefs and online activity.[9]

Investigation into a traveler's contacts and connections will expose many other US citizens to scrutiny, as well. Visitors from overseas, including from the seven Muslim-majority countries that are the subject of the enjoined travel ban, often have family, friends, and colleagues in the United States. These US citizens will also be exposed to CBP's "extreme vetting" of travelers' social networks and online contacts. They will become wary of engaging in their own online activity, for fear that something they tweet, like, or share will lead to them being detained at the airport the next time they travel. And it may undermine US citizens' willingness to make connections to other people, at home and abroad, given the risk of guilt by association with someone else's social media feed.

For all of these reasons, we urge you, Secretary Kelly, to reject any proposal to require passwords as a condition of entry into the United States and to cease the invasive examination of people's online activity at the border. We also seek the opportunity to meet with you and key agency personnel responsible for implementing these policies to discuss our concerns in further detail.

Sincerely,

Access Now
American Civil Liberties Union
American Library Association
American Society of Journalists and Authors
American Society of News Editors
American-Arab Anti-Discrimination Committee
Americans for Immigrant Justice
Association of Alternative Newsmedia
Association of Research Libraries
Bill of Rights Defense Committee/Defending Dissent Foundation
Brennan Center for Justice at NYU School of Law
Center for Democracy & Technology
Coalition for Humane Immigrant Rights of Los Angeles

---

[8] *See, e.g.*, Tresa Baldas, Detroit Free Press, "Travelers' texts, emails searched at Detroit Metro Airport," Jan. 30, 2017, http://www.freep.com/story/news/local/michigan/wayne/2017/01/30/travelers-texts-emails-searched-detroit-metro-airport/97257722/.

[9] The Council on Islamic-American Relations in Florida published a list of questions asked by CPB officers to Muslim-Americans, including "Are you a devout Muslim?" and "What social media accounts do you use?". "CAIR-FL Files 10 Complaints with CBP After the Agency Targeted and Questioned American-Muslims About Religious and Political Views", Jan. 18, 2017, https://www.cairflorida.org/newsroom/press-releases/720-cair-fl-files-10-complaints-with-cbp-after-the-agency-targeted-and-questioned-american-muslims-about-religious-and-political-views.html.

Comic Book Legal Defense Fund
Committee to Protect Journalists
The Constitution Project
Consumer Action
Council on American-Islamic Relations
Diversity-Immigration Committee of ATLI (Action Together Long Island)
Electronic Frontier Foundation
Free Speech Coalition
Future of Privacy Forum
Global Network Initiative
Human Rights First
Human Rights Watch
Immigrant Legal Resource Center
Interactive Advertising Bureau
Internews
Legal Aid Justice Center (Virginia)
Media Freedom Foundation
National Coalition Against Censorship
National Hispanic Media Coalition
National Organization for Women (NOW) New York State
New America's Open Technology Institute
Online Trust Alliance
PEN America
Project Censored
Public Knowledge
Reporters Without Borders
Resilient Communities Program, New America
Restore the Fourth
United Church of Christ, OC Inc.
World Privacy Forum
Wickr Foundation