The Heritage Foundation

ISSUE BRIEF

No. 4681 | APRIL 12, 2017

The U.S. Should Tread Carefully on Social Media Vetting

David Inserra

The Trump Administration and Congress are looking at social media screening as a method of detecting terrorists trying to come to the U.S. Social media screening is likely to be of little value and consume resources better spent elsewhere in the U.S. counterterrorism enterprise. Depending on how these searches are done, they also raise the prospect of serious cybersecurity concerns and detrimental repercussions for American citizens travelling abroad. The U.S. should carefully consider the usefulness of broad social media vetting before proceeding further.

Social Media and Terrorism

The use of social media tools ranging from Twitter to encrypted communications enabled on platforms like Facebook chat are well documented as supporting terrorist propaganda, recruiting, radicalization, and communication. For example, in mid-2015, ISIS created 38 unique propaganda pieces per day on social media, focusing on various themes such as victimhood, war, and utopia, with lesser themes including mercy, belonging, and brutality.[1] The messages on ISIS's social media campaign are reaching far and wide: At least 300 U.S.-based ISIS sympathizers were active on Twitter in 2015.[2]

To be clear, social media is not the reason terrorists radicalize; it is a tool used to spread a violent ideology faster and wider than traditional in-person networks. Social media campaigns supplementing face-to-face recruiting efforts have attracted thousands of foreign fighters to ISIS's cause from across the world with at least 25,000 foreign fighters as of late 2015.[3] This total includes thousands from the West and at least 250 from the U.S.—figures that will all have grown over the past year and half.

The U.S. has faced at least 25 attempted or successful Islamist terrorist attacks on home soil in the past several years that were at least inspired by ISIS.[4]

Social Media Screening as a Counterterrorism Tool

Given the role that social media has played in spreading ISIS's and other Islamist terror organization's apocalyptic vision for the future, screening social media seems an attractive way to find potential terrorists.

- Secretary of State Rex Tillerson has ordered consular officials responsible for conducting visa interviews to undertake "mandatory social media check[s] for applicants present in a territory at the time it was controlled by ISIS."[5]

- Secretary of Homeland Security John Kelly has commented: "We may want to get on their social media, with passwords" for individuals from "the seven countries" originally facing a temporary travel ban into the U.S.[6]

This paper, in its entirety, can be found at
http://report.heritage.org/ib4681

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

- Under President Obama, the Department of Homeland Security (DHS) was considering asking for social media information and started several pilot programs to see how to gather and use social media information as part of the vetting process.[7]

Congress has expressed interest in social media vetting, with several members introducing legislation to require it.[8]

Social media certainly does contain information that can help authorities; however, the devil is in the details. When vetting an individual's social media accounts, the U.S. government may find it difficult to find trustworthy information. A terrorist may provide visa or border officials with an incomplete or false list of his accounts that hides terrorist activity.

Meanwhile, other honest visa applicants will be providing officials with their social media information, which will take time to sort through. If officials cannot trust self-reported data, then they will need to search public, open-source social media and try to identify the accounts that may belong to a traveler. The DHS inspector general identified challenges in DHS's pilots with matching social media accounts to travelers and being sure the travelers were providing all of their accounts.[9]

Collecting all this additional information is helpful if officials believe it will help them identify the needle in the haystack, but it can be counterproductive if it only adds more hay for officials to sort through.

One benefit of using social media as part of the vetting process is the ability to use false statements against dishonest travelers. If the U.S. discovers that a traveler to the U.S. did not provide his full and correct set of social media accounts, then that false statement can be used to prevent his entry, prosecute him, or deport him.

Unintended Consequences of Social Media Vetting

Beyond its imperfect role in stopping terrorist entry, social media vetting, especially when requiring passwords, is ripe for such harmful unintended consequences as the following:

- **Account compromise.** From a cybersecurity perspective, if DHS or the State Department are going to be gathering social media passwords for travelers around the world, the chances of these accounts being compromised increases. Social media passwords would be a target for hacktivists, criminals, and nation-state actors. Given incidents like the breach of the Office of Personnel Management, travelers to the U.S. would have significant reason to be concerned.

[1] Charlie Winter, "Documenting the Virtual 'Caliphate,'" Quilliam, October 2015, http://truevisiontv.com/uploads/websites/39/wysiwyg/doctors/jihad/FINAL-documenting-the-virtual-caliphate.pdf (accessed April 5, 2017).

[2] Lorenzo Vidino and Seamus Hughes, "ISIS in America," Program on Extremism, The George Washington University, December 2015, https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf (accessed April 5, 2017).

[3] Lisa Curtis, Luke Coffey, David Inserra, Daniel Kochis, Walter Lohman, Joshua Meservey, James Phillips, and Robin Simcox, "Combatting The ISIS Foreign Fighter Pipeline: A Global Approach," Heritage Foundation *Special Report* No. 180, January 6, 2016, http://www.heritage.org/middle-east/report/combatting-the-isis-foreign-fighter-pipeline-global-approach.

[4] Riley Walters, "Kansas City Bombing Scheme Becomes First Terror Plot of 2017," The Daily Signal, March 6, 2017, http://dailysignal.com/2017/03/06/kansas-city-bombing-scheme-becomes-first-terror-plot-of-2017/.

[5] Yeganeh Torbati, Mica Rosenberg, and Arshad Mohammed, "Exclusive: U.S. Embassies Ordered to Identify Population Groups for Tougher Visa Screening," Reuters, March 23, 2017, http://live.reuters.com/Event/Live_US_Politics/791255396 (accessed April 5, 2017).

[6] "DHS Chief Says US Might Ask Visa Applicants for Social Media Passwords," Fox News, February 8, 2017, http://www.foxnews.com/politics/2017/02/08/dhs-chief-says-us-might-ask-visa-applicants-for-social-media-passwords.html (accessed April 5, 2017).

[7] Office of the Inspector General, "DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success," U.S. Department of Homeland Security, February 27, 2017, https://www.oig.dhs.gov/assets/Mgmt/2017/OIG-17-40-Feb17.pdf (accessed April 5, 2017).

[8] Ron Nixon, "Visitors to the U.S. May Be Asked for Social Media Information," *The New York Times*, June 28, 2016, https://www.nytimes.com/2016/06/29/us/homeland-security-social-media-border-protection.html (accessed April 5, 2017), and Heather Kuldell, "Lawmakers Want Social Media Vetted for All Visa Applicants and Ask More Mar-A-Lago Questions," Nextgov, February 17, 2017, http://www.nextgov.com/cio-briefing/2017/02/lawmakers-want-social-media-vetted-all-visa-applicants-and-ask-more-mar-lago-questions/135558/ (accessed April 5, 2017).

[9] Office of the Inspector General, "DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success."

- **Retaliatory or reciprocal actions.** An additional cybersecurity and privacy concern is that if the U.S. begins to widely demand social media passwords from foreign travelers, other countries with less concern for security and privacy may demand passwords from U.S. travelers. This is not to say that the U.S. cannot request this information from foreigners (the U.S. has the right to request this information as a condition for entry to the U.S.), but the request may be unwise because of retaliatory or reciprocal actions taken by other countries.

- **Potential waste of resources.** A final unintended consequence of such an action is that it consumes limited counterterrorism and vetting funding. Finding accurate social media information for visitors will either require more funding or take away some resources from existing vetting and counterterrorism operations. Given that since the start of 2015, all 30 Islamists plots and attacks against the U.S. homeland have involved a homegrown terrorist, the U.S. must not shift resources away from countering such threats in order to start broad social media vetting efforts.

Protecting the Homeland from Terrorism

Given the role of social media in today's terrorism, the U.S. must develop policies that collect and analyze social media data so it can reliably be used by U.S. law enforcement, immigration, and intelligence officials. Congress and the Administration should:

- **Investigate the usefulness of social media information before mandating its widespread use.** Requesting social media accounts can be used to prosecute or punish those who make false statements. Asking all travelers to self-report social media accounts and passwords, however, can be evaded while creating whole new data security problems. On the other hand, searching publically available social media accounts will require a great deal of work to sort through largely benign accounts. The cost-effectiveness of social media vetting must be considered before it is broadly used.

- **Start with targeted use of social media.** DHS should start with targeted requests for social media information paired with searches of social media platforms to supplement vetting tools on higher risk applicants.

- **Focus on the homeland.** While vetting can and should always be improved, the U.S. must not lose sight of homegrown terrorists, the primary Islamist terrorist threat the homeland has faced over the past decade. Intelligence tools and resources for the FBI, improved information sharing between local law enforcement and the FBI, properly focused counter-radicalization efforts, and other such policies are needed to stop terrorists already present in the U.S.

Policies That Keep America Safe

The use of social media as a tool by terrorists to communicate is widespread and policymakers are rightly wondering what can be done to use these communications in U.S. vetting efforts. The U.S. should explore how it can use social media in a cost-effective and targeted manner to enhance U.S. security while remaining focused on the homegrown Islamist terrorism threat.

*—**David Inserra** is Policy Analyst for Homeland Security and Cyber Security in the Douglas and Sarah Allison Center for Foreign Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*