

WHAT A SOCIAL MEDIA CHECK FOR VISAS WOULD REQUIRE

There's a bunch of fevered commentary arising out of the report that Tashfeen Malik, one of the perpetrators of the San Bernardino attack, espoused extremism on Facebook before she entered the country. Otherwise sane members of Congress are submitting legislation calling for the government to review social media before granting a visa.

Here's why that's dumb.

First, let's look at whether the State Department really could have found Malik's posting before granting her a K1 visa. As CNN reported, Malik *hadn't* actually been plotting jihad in the open, as much of the reporting on this suggests.

Tashfeen Malik advocated jihad in messages on social media, but her comments were made under a pseudonym and with strict privacy settings that did not allow people outside a small group of friends to see them, U.S. law enforcement officials told CNN on Monday.

[snip]

The New York Times reported on Sunday that U.S. immigration officials conducted three background checks on Malik when she emigrated from Pakistan but allegedly did not uncover social media postings in which she said she supported violent jihad and wanted to be a part of it.

According to the law enforcement officials, because Malik used a pseudonym and privacy controls, her postings would not have been found even

if U.S. authorities had reviewed social media as part of her visa application process.

A U.S. official told CNN shortly after the San Bernardino attack that the United States only recently began reviewing the social media activity of visa applicants from certain countries. The date that these types of reviews began is not clear, but it was after Malik was considered, the source said.

So to get to the posts in question, someone would have had to match her pseudonym to a known identifier of hers, access her private communication, and then translate it from Urdu.

The NSA (though not State) actually has the ability to do that. They'd probably find her pseudonym either the way the FBI reportedly did, by giving Facebook her known email which they'd find was tied to that account, or they'd stick known identifiers (including name, email, credit card with which she paid her visa fee) into a tool the NSA has for correlating identities.

This process would be helped, of course, if DHS' online visa application system was working, because that would not only increase the chances you'd get a working email for the applicant, but it would also give you at least one IP address you could also correlate on. But the effort to do that has become the worst kind of boondoggle, with a billion dollars spent and just one online form working. So this whole process would be started with less certainty attached to any online identifier.

The NSA also has the ability to read private posts – on Facebook at least. Given that at the time Malik applied for her visa she was *neither* a US person (I'm still not certain whether she would have been treated as a US person just with a fiance visa, on application for a Green Card, or on receipt of one), *nor* in

the country, NSA could have used PRISM (with the added benefit that it would provide a bunch more identities to check).

Of course, you'd also want to check non-US social media, like Telegram (which ISIS has reportedly been using) and Vkontakte (which the Tsarnaev brothers used). That's going to be harder to do.

Finally, you'd have to translate any posts Malik wrote from Urdu to English. While an initial translation could be done by machine, to understand any subtleties of the posting, you'd need to get a human translator to do the work, and even for key languages like Urdu and Arabic, the government has far too few translators.

So you could do such a check, at least for US-based social media, but you'd have to involve the NSA.

Now consider the resource demands of doing this. There are upwards of 450,000 immigrant visas issued each year. There are another 750,000 student and temporary work visas, both categories of which are closer to a typical terrorist profile than a fiance visa (that doesn't include exchange visitors and a range of other kinds of work visas).

Last year, the government targeted 92,000 people under Section 702, which you'd have to use to get just private (not encrypted) communications. So you'd have to do an order of magnitude more PRISM searches every year to thoroughly check the social media of just the most obvious visa applicants. You'd either have to vastly expand NSA's workforce – and require key social media providers, like Facebook, to do the same just to stay ahead of compliance requests – or you'd have to pull them off of investigating targets about which they have some reason to be interested already.

Of course, if you did that – if you passed a law requiring all immigrants and long term visa applicants to be checked – then you'd make it far easier for people to evade detection,

because you'd be alerting the few people who'd want to evade detection that you would check their accounts. They could then move to social media, like Telegram, that the US would have a harder time checking, and encrypt their messages.

Moreover, you'd be making this great effort at a time when much more obvious problems (such as that online form!) haven't been fixed. Most importantly, since 9/11, it has been a top priority to track the exits of short term visitors (including those people with visa waivers), and the government still hasn't managed that yet. If you want to make America more safe, you'd be far better served finally fixing that problem than reading a million people's secret social media posts.