

BREAKING! THERE WERE STATE-SPONSORED TERRORISTS OPERATING IN THE US IN 2015

If we're to believe the NYT's explanation for why Yahoo was asked to scan all its email in 2015, there are (or were) state-sponsored terrorists operating in the US. That's the only logical explanation for why the FBI would use an individualized FISA court order to obligate Yahoo to adapt their kiddie porn filter to search for a signature used by what NYT describes as state sponsored terrorists.

Although the digital signature was individually approved by a judge, who was persuaded that there was probable cause to believe that it was uniquely used by a foreign power, the collection was unusual because it involved the systematic scanning of all Yahoo users' emails. More typical surveillance court orders instead target specific user accounts.

[snip]

In fact, according to the government official and other people familiar with the matter, Yahoo was served with an individualized court order to look only for code uniquely used by the foreign terrorist organization, and it adapted the scanning systems that it already had in place to comply with that order rather than building a new capability.

Now, I don't find this explanation all that plausible, because if there were *real* state-sponsored terrorists operating in the US, the US would be bombing the shit out of the country in question. Pakistan and Saudi Arabia sponsor terrorists, but they're our friends and we try

to overlook the way they foster terrorism. So I'm betting these aren't real terrorists, but instead entities the government has told the FISA Court are terrorists to make it possible to approve things they otherwise would find questionable. Plus, it sounds so much cooler when you make such explanations than if you admit you were scanning all Yahoo users' emails to search for hackers.

I'm going to wildarseguess that this really means the US had a line on Iranian Revolutionary Guard hacking techniques. I say that because the government has long argued that Iran (or at least, the Revolutionary Guard) is a terrorist organization so it can use fancy spy tools that have only been approved for terrorism uses. It's a bullshit claim, but one the FISC has consistently approved going back years, probably to 2006 (and one OLC almost certainly approved under Stellar Wind). If this operation had happened two months later, after USA Freedom Act expanded the definition of foreign power to within two degrees of proliferators, they might have used that excuse, but back then, piggybacking a terrorist claim onto the use of the foreign government tie would provide the most impressive claim to need to scan domestically.

We even know the IRGC uses Yahoo, because that's what NSA was collecting on in 2011 when someone spamouflaged key IRGC accounts at precisely the moment we weretrying to entrap a top IRGC commander in the Scary Iran Plot.

And while the request to Yahoo came at a later time, we know that the US was aggressively going after Iranian hackers at least in late 2014 because they were targeting banks. DOJ would go on to indict a bunch of Iranians for, among other things, hacking a very small dam.

So rest assured, Yahoo users! FBI only made Yahoo scan your emails because it was hunting terrorists in your inbox.

But remember, that also means there are real

state-sponsored terrorists – and not just ISIS wannabes – among us.

Update: Revolutionary for Republican fixed.