THE YAHOO SCANS CLOSELY FOLLOWED OBAMA'S CYBERSECURITY EMERGENCY DECLARATION

Reuters has a huge scoop revealing that, in spring of 2015, Yahoo was asked and agreed to perform scans for certain selectors on all the incoming email to its users.

> The company complied with a classified U.S. government directive, scanning hundreds of millions of Yahoo Mail accounts at the behest of the National Security Agency or FBI, said two former employees and a third person apprised of the events.
>
> [snip]
>
> It is not known what information intelligence officials were looking for, only that they wanted Yahoo to search for a set of characters. That could mean a phrase in an email or an attachment, said the sources, who did not want to be identified.

The timing of this is particularly interesting. We know that it happened sometime in the weeks leading up to May 2015, because after Alex Stamos' security team found the code enabling the scan, he quit and moved to Facebook.

> According to the two former employees, Yahoo Chief Executive Marissa Mayer's decision to obey the directive roiled some senior executives and led to the June 2015 departure of Chief Information Security Officer Alex Stamos, who now holds the top security job at Facebook

> Inc.
>
> [snip]
>
> The sources said the program was discovered by Yahoo's security team in May 2015, within weeks of its installation. The security team initially thought hackers had broken in.
>
> When Stamos found out that Mayer had authorized the program, he resigned as chief information security officer and told his subordinates that he had been left out of a decision that hurt users' security, the sources said. Due to a programming flaw, he told them hackers could have accessed the stored emails.

That would date the directive to sometime around the time, on April 1, 2015, that Obama issued an Executive Order declaring cyberattacks launched by persons located outside the US a national emergency.

> I, BARACK OBAMA, President of the United States of America,find that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside theUnited States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of theUnited States. I hereby declare a national emergency to deal with this threat.

On paper, this shouldn't create any authority to expand surveillance. Except that we know FISC did permit President Bush to expand surveillance — by eliminating the wall between intelligence and criminal investigations — after he issued his September 14, 2001 9/11 emergency declaration, before Congress authorized that expansion. And we know that Jack Goldsmith focused on that same emergency declaration in

his May 2004 OLC opinion reauthorizing Stellar Wind.

Indeed, just days after Obama issued that April 2015 EO, I wrote this:

> Ranking House Intelligence Member Adam Schiff's comment that Obama's EO is "a necessary part of responding to the proliferation of dangerous and economically devastating cyber attacks facing the United States," but that it will be "coupled with cyber legislation moving forward in both houses of Congress" only adds to my alarm (particularly given Schiff's parallel interest in giving Obama soft cover for his ISIL AUMF while having Congress still involved). It sets up the same structure we saw with Stellar Wind, where the President declares an Emergency and only a month or so later gets sanction for and legislative authorization for actions taken in the name of that emergency.
>
> And we know FISC has been amenable to that formula in the past.
>
> We don't know that the President has just rolled out a massive new surveillance program in the name of a cybersecurity Emergency (rooted in a hack of a serially negligent subsidiary of a foreign company, Sony Pictures, and a server JP Morgan Chase forgot to update).
>
> We just know the Executive has broadly expanded surveillance, in secret, in the past and has never repudiated its authority to do so in the future based on the invocation of an Emergency (I think it likely that pre FISA Amendments Act authorization for the electronic surveillance of weapons proliferators, even including a likely proliferator certification under Protect America Act,

> similarly relied on Emergency Proclamations tied to all such sanctions).
>
> I'm worried about the Cyber Intelligence Sharing Act, the Senate version of the bill that Schiff is championing. But I'm just as worried about surveillance done by the executive prior to and not bound by such laws.
>
> Because it has happened in the past.

I have reason to believe the use of emergency declarations to authorize surveillance extends beyond the few data points I lay out in this post. Which is why I find it very interesting that the Yahoo request lines up so neatly with Obama's cyber declaration.

I'm also mindful of Ron Wyden's repeated concerns about the 2003 John Yoo common commercial services opinion that may be tied to Stellar Wind but that, Wyden has always made clear, has some application for cybersecurity. DOJ has already confirmed that some agencies have relied on that opinion.

In other words, this request may not just be outrageous because it means Yahoo is scanning all of its customers incoming emails. But it may also be (or have been authorized by) some means other than FISA.