

SINCE SEPTEMBER 20, 2012, FBI HAS BEEN PERMITTED TO SHARE FISA-DERIVED HACKING INFORMATION WITH INTERNET SERVICE PROVIDERS

As I noted, yesterday Reuters reported that in 2015, Yahoo had been asked to scan its incoming email for certain strings. Since that time, Yahoo has issued a non-denial denial saying the story is “misleading” (but not wrong) because the “mail scanning described in the article does not exist on our systems.”

As I suggested yesterday, I think this most likely pertains to a cybersecurity scan of some sort, in part because FISC precedents would seem to prohibit most other uses of this. I’ve addressed a lot of issues pertaining to the use of Section 702 for cybersecurity purposes here; note that FISC might approve something more exotic under a traditional warrant, especially if Yahoo were asked to scan for some closely related signatures.

If you haven’t already, you should read my piece on why I think CISA provided the government with capabilities it couldn’t get from a 702 cyber certificate, which may explain why the emphasis on present tense from Yahoo is of particular interest. I think it quite likely tech companies conduct scans using signatures from the government now, voluntarily, under CISA. It’s in their best interest to ID if their users get hacked, after all.

But in the meantime, I wanted to point out this language in the 2015 FBI minimization procedures which, according to this Thomas Hogan opinion (see footnote 19), has been in FBI minimization

procedures in some form since September 20, 2012, during a period when FBI badly wanted a 702 cyber certificate.

The FBI may disseminate FISA-acquired information that ... is evidence of a crime and that it reasonably believes may assist in the mitigation or prevention of computer intrusions or attacks to private entities or individuals that have been or are at risk of being victimized by such intrusions or attacks, *or to private entities or individuals (such as Internet security companies and Internet Service Providers) capable of providing assistance in mitigating or preventing such intrusions or attacks.* Wherever reasonably practicable, such dissemination should not include United States person identifying information unless the FBI reasonably believes it is necessary to enable the recipient to assist in the mitigation or prevention of computer intrusions or attacks. [my emphasis]

This is not surprising language: it simply permits the FBI (but not, according to my read of the minimization procedures, NSA) to share cyber signatures discovered using FISA with private sector companies, either to help them protect themselves or because private entities (specifically including ISPs) might provide assistance in mitigating attacks.

To be sure, the language falls far short of permitting FBI to demand PRISM providers like Yahoo to use the signatures to scan their own networks.

But it's worth noting that Thomas Hogan approved a version of this language (extending permitted sharing even to physical infrastructure and kiddie porn) in 2014. He remained presiding FISA judge in 2015, and as such would probably have reviewed any exotic or new programmatic

requests. So it would not be surprising if Hogan were to approve a traditional FISA order permitting FBI (just as one possible example) to ask for evidence on a foreign-used cyber signature. Sharing a signature with Yahoo – which was already permitted under minimization procedures – and asking for any results of a scan using it would not be a big stretch.

There's one more detail worth remembering: way back the last time Yahoo challenged a PRISM order in 2007, there was significant mission creep in the demands the government made of Yahoo. In August 2007, when Yahoo was initially discussing compliance (but before it got its first orders in November 2007), the requests were fairly predictable: by my guess, just email content. But by the time Yahoo started discussing actual compliance in early 2008, the requests had expanded, apparently to include all of Yahoo's services (communication services, information services, storage services), probably even including information internal to Yahoo on its users. Ultimately, already in 2008, Yahoo was being asked to provide nine different things on users. Given Yahoo's unique visibility into the details of this mission creep, their lawyers may have reason to believe that a request for packet sniffing or something similar would not be far beyond what FISC approved way back in 2008.