HOW CISA MIGHT HURT FBI'S ABILITY TO FIGHT CYBERATTACKS

DOJ's Inspector General just released a report on how well FBI's cybersecurity initiative has been going. In general, it finds that the FBI has improved its ability to investigate cyberattacks.

But among the most significant challenges facing the FBI is in two-way information sharing with the private sector.

You might think that the Cyber Information Sharing Act — which after all, aims to increase information sharing between the private sector and those in government who will investigate it — would help that.

On one count it would: private sector entities interviewed by the IG were reluctant to cooperate with the FBI because of FOIA concerns.

> During our interviews with private sector individuals, we found that private sector entities are reluctant to share information, such as PII or sensitive or proprietary information, with the government because of concerns about how that information could be used or the possibility that it could be publicly released under the Freedom of Information Act (FOIA).26 One private sector professional told us that he had declined to be interviewed by the OIG due to FOIA concerns.

CISA would include a blanket exception from FOIA — which is not necessarily a good thing, but should placate those who have these concerns.

But other private sector entities expressed concerns about the multiple uses to which shared data would be put. They cited Snowden disclosures showing data might be used for other

purposes.

> In addition, several private sector individuals discussed with us the challenges in collaborating with the FBI in a "post-Snowden" era. One private sector individual emphasized that Snowden has redefined how the private sector shares information with the United States government. We were told by private industry representatives and the FBI that, following the Snowden disclosures, private sector entities have become more reluctant to share information with the United States government because they are uncertain as to how the information they provide will be used and are concerned about balancing national security and individual privacy interests.

The recent reports on the use of cyber signatures for upstream Section 702 collection show that the NSA and FBI might be able to use signatures to search all traffic (though I suspect FISC has put more limitations on this practice than is currently known).

Just as troubling, however, are the broad permissions under CISA to use the data turned over under the law for prosecutions on a range of crimes. Right now, ECPA has provided tech companies — at least the ones that pushed back on NSLs demanding Internet data — a way to protect their customers from fishing expeditions. CISA is voluntary (though I can imagine many ways pressure would be brought to participate), but it does undermine that system of protections for customers.

When commenting on this, Jim Comey apparently added in proprietary information among the concerns of providers, along with the explicitly described "guard[ing] customer data.

> The FBI Director has acknowledged private sector concerns related to

> proprietary information and the need to guard customer data and stated the FBI will do what it can to protect private sector privacy.27

Given NSA's voracious use of any information it gets its hands on, and the broad permissions for information sharing in the bill, the protections for trade secrets may not be enough for the private sector, since it's now clear the government, not just competitors, is exploiting trade secrets.

The IG ends this section urging the FBI to provide "appropriate assurances" about its handing of Personally Identifiable Information.

> More generally, efforts to detect, prevent, and mitigate threats are hampered because neither the public nor private sector can see the whole picture.
>
> The FBI Director further explained government lacks visibility into the many private networks maintained by companies in the United States, and the FBI "has information it cannot always share [with the private sector]." Consequently, each can see distinct types of cyber threats, but the information is not always visible to the other. We believe that the FBI should strengthen its outreach efforts to provide appropriate assurances regarding its handling of PII and proprietary information received from the private sector and work to reduce classification, where appropriate, of information in its possession in order to improve sharing and collaboration in both directions consistent with appropriate privacy and other limitations.

It is just my opinion, but I suspect CISA, as

written, would further exacerbate concerns.

Finally, Inspector General Michael Horowitz' statement releasing this report includes something not developed in the report itself, perhaps because it is a more recent concern: security of data shared with the federal government.

> And, the FBI continues to face challenges relating to information sharing with private sector entities, in part because of concerns in the private sector about privacy *and the security of sensitive information* it shares with the government.

I'd be very interested in whether this stems just from trade secret concerns or from the concern that several of the agencies that would automatically get data shared with the government have their own cybersecurity challenges.