ON CISA THE SURVEILLANCE BILL

After the Senate Intelligence Committee passed CISA, its sole opponent, Ron Wyden, said, "If information-sharing legislation does not include adequate privacy protections then that's not a cybersecurity bill – it's a surveillance bill by another name." Robert Graham, an expert on intrusion-prevention, argues, "This is a bad police-state thing. It will do little to prevent attacks, but do a lot to increase mass surveillance."

Clearly, some people who have reason to know think this bill doesn't do what it says, but instead does a lot of what it isn't admitting.

I want to look at several aspects of the bill from that perspective (this post primarily deals with the SSCI version but the HPSCI version is very similar).

Can our ISPs take countermeasures against us?

First, whom it affects. Ron Wyden has been warning about the common commercial service OLC memo and its impact on the cybersecurity debate for years, suggesting that still secret memo conflicted public's understanding of "the law" (though he doesn't say what law that is). While it's unclear what that OLC memo says, Wyden seems to suggest that Americans have been subject to cybersecurity surveillance that they didn't know about (perhaps because OLC had interpreted consent where it didn't exist).

So I think it's important that at the center of a series of definitions of "entities" in CISA is a definition that would include us, as private entities.

> IN GENERAL.—Except as otherwise provided in this paragraph, the term ''private entity'' means any person or private

> group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

That's important because the law permits both monitoring…

> (1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—
>
> (A) an information system of such private entity;
>
> (B) an information system of another entity, upon the authorization and written consent of such other entity;

And defensive measures (what the bill has renamed the largely otherwise indistinguishable "countermeasures") against a private entity that has provided consent to another private entity.

> (B) EXCLUSION.—The term ''defensive measure'' does not include a measure that destroys, renders unusable, or substantially harms an information system or data on an information system not belonging to—
>
> (i) the private entity operating the measure; or
>
> (ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

At a minimum, I think this should raise questions about whether Terms of Service of cable companies and Internet Service Providers and banks and telecoms amount to consent for this kind of monitoring and — in the name of

cybersecurity — countermeasures.

Researching more crimes in name of cybersecurity than in name of terror

This is important, because CISA actually permits the use of information collected in the name of "cybersecurity" to be used for more uses than the NSA is permitted to refer it under foreign intelligence collection (though once FBI is permitted to back door search everything, that distinction admittedly disappears). In addition to its use for cybersecurity — which is itself defined broadly enough to mean, in addition, leak and Intellectual Property policing — this "cybersecurity" information can be used for a variety of other crimes.

> (iv) the purpose of responding to, or otherwise preventing or mitigating, an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction;
>
> (v) the purpose of responding to, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or
>
> (vi) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iv) or any of the offenses listed in— (I) section 3559(c)(2)(F) of title 18, United States Code (relating to serious violent felonies); (II) sections 1028 through 1030 of such title (relating to fraud and identity theft); (III) chapter 37 of such title (relating to espionage and censorship); and (IV) chapter 90 of such title (relating to protection of trade secrets).

As a number of people have noted, for CISA data to be used for the purposes suggest both private entities – upon sharing – and the government – on intake – actually will be leaving a fair amount of data in place.

Why does domestic spying have less stringent minimization than foreign spying?

Which brings me to the purported "privacy and civil liberties guidelines" the bill has. The bill mandates that the Attorney General come up with guidelines to protect privacy that will,

> (A) limit the impact on privacy and civil liberties of activities by the Federal Government under this Act;
>
> (B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or identifying specific persons, including by establishing–
>
> > (i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this Act; and
> >
> > (ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;
>
> (C) include requirements to safeguard cyber threat indicators containing personal information of or identifying specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;
>
> (D) include procedures for notifying

> entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;
>
> (E) protect the confidentiality of cyberthreat indicators containing personal information of or identifying specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this Act; and
>
> (F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

It's worth comparing what would happen here to what happens under both Section 215 (which FBI claims to use for cybersecurity) and FAA (which ODNI has admitted to using for cybersecurity — and indeed, which uses upstream searches to find the very same kind of signatures).

With the former, the FISC had imposed minimization procedures and required the government report on compliance with them. The FISC, not the AG, has set retention periods. And at least for the NSA's use of Section 215 (which should be the comparison here, since NSA will be one of the agencies getting the data), data must be presumptively minimized. Also, unlikely the phone dragnet data, at least, where data must be certified according to a counterterrorism use, here, data is shared across multiple agencies in real time.

FAA's minimization procedures also get reviewed by the FISC (though reports back are probably not as stringent, though they are checked yearly). And there's a whole slew of reporting.

While there is some reporting here, it is

bifurcated so that PCLOB, which has no subpoena power, does the actual privacy assessment, whereas the Inspectors General, which are assured they can get information they need (even if DOJ's Inspector General keeps getting denied data they should get), report solely on numbers and types of usage, without a privacy or even compliance assessment.

One of my favorite parts of CISA (this is true of both bills) is that while the bills mandate an auditing ability, they don't actual mandate audits (the word appears exactly once in both bills).

In other words, Congress is about to adopt a more permissive collection of data for domestic spying than it does for foreign spying. Or, in the context of Section 215, it may be adopting more permissive treatment of data voluntarily turned over to the government than that data turned over in response to an order.

And all that's before you consider data flowing in the reverse direction. While the bills do require penalties if a government employee or agent (which hopefully includes the contractors this bill will spawn) abuses this data sharing, it does not for private entities. (The House version also has a 2 year statute of limitations for this provision, which all but guarantees it will never be used, given that it would never be discovered in that period, particularly given the way FOIA and Trade Secret exemptions make this data sharing less accessible even than spying data.)

Perhaps my very favorite part of this bill appears only in the House version (which of course came after the Senate version elicited pretty universal complaints that it was a surveillance bill from civil libertarians). It has several versions of this clause.

> (a) PROHIBITION OF SURVEILLANCE.—Nothing in this Act or the amendments made by this Act shall be construed to authorize the Department of Defense or the

> National Security Agency or any other element of the intelligence community to target a person for surveillance.

The word “surveillance,” divorced from the modifier “electronic” is pretty meaningless in this context. And it’s not defined here.

So basically HPSCI, having seen how many people correctly ID this as a surveillance bill, has just taken a completely undefined term “surveillance” and prohibited that under this bill. So you can collect all the content you want under this bill with no warrant, to you can supersede ECPA all you want too, but just don’t call it surveillance.