Cyber Intelligence Bill Threatens Privacy and Civilian Control

by Greg Nojeim [1]
December 1, 2011

A bill unveiled yesterday by Reps. Mike Rogers (R-MI) and C.A. “Dutch” Ruppersberger (D-MD), the Chairman and Ranking Member of the House Intelligence Committee, would authorize Internet service providers and other companies to share customer communications and other personally identifiable information with governmental agencies. The intent of the bill is to enhance information sharing for cybersecurity purposes, a goal that CDT strongly supports. However, we have four main concerns with the specifics of the Rogers-Ruppersberger bill:

- The bill has a very broad, almost unlimited definition of the information that can be shared with government agencies notwithstanding privacy and other laws;
- The bill is likely to lead to expansion of the government’s role in the monitoring of private communications as a result of this sharing;
- It is likely to shift control of government cybersecurity efforts from civilian agencies to the military;
- Once the information is shared with the government, it wouldn’t have to be used for cybersecurity, but could instead be used for any purpose that is not specifically prohibited.

The bill, titled the Cyber Intelligence Sharing and Protection Act, is on a fast track – the House Intelligence Committee has scheduled the bill for mark up today.

Relationship to the “DIB Pilot:” The legislation is being billed as an expansion of a collaboration between the National Security Agency (NSA) and major ISPs dubbed the Defense Industrial Base Pilot. Under the DIB Pilot, the NSA shares classified cyberattack signatures and information about cybersecurity threats with large ISPs that provide Internet service to major defense contractors. Under their service agreements with those contractors, the ISPs use the NSA signatures, and other cyberattack signatures that the ISPs have developed or otherwise obtained, to scan communications to the defense contractors in order to screen out malware and other attacks. Under the DIB Pilot as initially implemented, the ISPs tell the defense contractors what communications have been blocked or flagged as suspicious, but the ISPs do not share traffic with the NSA.

If the bill merely extended to other companies the opportunity to receive classified attack signatures from the NSA so they could better defend their networks, CDT would actively support the legislation. Indeed, we have called this aspect of the DIB Pilot an “elegant solution” [2] that unlocks NSA knowledge to help the private sector defend itself.

However, the bill goes much further, permitting ISPs to funnel private communications and related information back to the government without adequate privacy protections and controls. The bill does not specify which agencies ISPs could disclose customer data to, but the structure and incentives in the bill raise a very real possibility that the National Security Agency or the DOD’s Cybercommand would be the primary recipient.

Unlike the DIB Pilot, the bill thus has two major implications that would radically change national cybersecurity policy:

(i) It could shift the center of cybersecurity efforts from the private sector to the government, making the government the hub for information sharing and analysis.

(ii) It could shift control of the government’s cybersecurity efforts from civilian control (now centered at the Department of Homeland Security) to the military.

Because the military cybersecurity agencies (NSA and Cybercommand) operate in secret, the bill could also undermine the transparency that is essential to public support for any cybersecurity program. Indeed, the bill would even permit the Director of National Intelligence to condition the sharing of classified cyberattack signatures and threat information on a company's agreement to share information back to the elements of the intelligence community.

How the bill would work: The bill encompasses three quite different kinds of information sharing, which pose very different considerations: sharing government information (attack signatures and other threat or vulnerability knowledge) with the private sector; sharing attack, threat and vulnerability information, including private communications data, among private sector companies for mutual self-protection; and sharing attack, threat and vulnerability information, including private communications data, with the government.

The first type of sharing is addressed in the section of the bill that authorizes the Director of National Intelligence to establish procedures through which companies could apply to become certified to receive cyberattack signatures and threat information from elements of the intelligence community. Once certified, a company could use that information for any purpose (except to gain an undefined "unfair competitive advantage"), including to protect its own network or the network of a company that had hired it to provide cybersecurity services.

The second and third kinds of information sharing are addressed in the provisions of the bill authorizing companies, whether certified or not, to use "cybersecurity systems" to obtain "cyberthreat information" and to share that information: (i) with other companies of their choosing subject to any limits the company authorizing the sharing might place; (ii) with any agency of their choosing in the Federal Government, but without any such use limits. Such sharing would be authorized even if otherwise barred by the electronic surveillance laws, other privacy statutes, or any other statutes at all.

Under the bill, when communications data is shared with the government, it could be used to prosecute an individual for any crime, used to target him or her for intelligence surveillance, and shared among governmental agencies to the extent permitted by current law and used by those agencies for any lawful non-regulatory governmental purpose. Data shared with other entities in the private sector could be used and redisclosed for any purpose, subject only to restrictions placed on such sharing by the entity authorizing the information to be shared – whether the authorizing entity is "self protected" or hires a "cybersecurity provider" such as an ISP. The bill itself places no limits on secondary use or dissemination of unclassified cyber threat information. Under the bill, the data can even be used to target advertising. Companies that in good faith share information impermissibly, or in good faith fail to act on information shared with them that reveals a vulnerability they leave unaddressed, are completely insulated from liability.

Much of the bill turns on definitions. The "cyber threat information" that a company is authorized to share is broadly defined as information

> … directly pertaining to a vulnerability of, or threat to a system or network of a government or private entity, including information pertaining to the protection of the system or network from—(A) efforts to degrade, disrupt or destroy such system or network; or (B) theft or misappropriation of private or government information, intellectual property or personally identifiable information.

This includes not only meta-data, but also the content of communications themselves. The information does not have to be limited to that pertaining to a known or suspected attack or activity indicative of a probe or attempted attack. Instead, it encompasses any information "pertaining to the protection of" a system or network. All systems and networks are included, not just those that hold classified information or control critical infrastructure. Since any message could contain an attack, and since carriers routinely scan all their traffic in "protecting" their networks, this could allow all of that traffic to be shared with the government. Since all log-in information retained by a social networking site or an online merchant "pertains" to protecting that system, all that information could be disclosed to the government as well. The bill would permit companies to share this information

without a court order for cybersecurity purposes with the National Security Agency, the FBI and any other government agency, which could then use the information for any purpose not otherwise illegal.

Inadequate privacy protections: In theory, there are three privacy protections in the bill, but each is toothless.

The first is a restriction on purpose: information can only be shared for a "cyber security purpose." But this protection is toothless because the definition of what can be shared is so broad and because cybersecurity does not have to be the sole or even primary purpose of the sharing. Moreover, once shared even for a legitimate cybersecurity purpose, the information could then be used for other non-regulatory purposes.

The second theoretical protection is that a company authorizing the sharing of information can put restrictions on further sharing that include anonymization and minimization of such information. This is toothless because it is voluntary with the company, and not enforceable by the users whose data can be shared.

The third is an annual report from the Privacy and Civil Liberties Oversight Board, which does not exist and hasn't existed for over three years. At any rate, a reporting requirement is no substitute for meaningful standards for information sharing.

Relationship with Republican Task Force Recommendations: Rather than faithfully implement the recommendations of the House Republican Cybersecurity Task Force, the bill in some ways stands in strong contrast to them.

- There is no requirement to minimize the personally identifiable information that is shared with the government, even though the Task Force called for such minimization.
- The Task Force, recognizing that overbroad legal protections for sharing information could harm privacy, said that "protection of personal privacy should be at the forefront of any limited legal protection proposal." Instead, there is no requirement in the bill to impose restrictions on information sharing that protect privacy. In fact, because companies are given blanket immunity if they share information in good faith, and are authorized to share that information notwithstanding any other law, their incentive to protect privacy is severely diminished.
- The information sharing would occur without the creation of the information clearinghouse outside of the government that the Task Force called for, and through which enforceable rules governing information sharing could be implemented.

Conclusion: We appreciate that the bill meets many of the needs that companies have been raising: it permits sharing between companies with very few restrictions while at the same time allowing companies to impose the restrictions they choose; it prohibits using shared information to regulate companies; and it provides immunity. However, these features are outweighed, significantly, by the extent to which the bill permits essentially unfettered sharing with the government and in particular with the military side of the government and by the fact that the DNI can use the certification process for government-to-private sharing in order to incentivize the private sector to share more with the military side of government without restrictions, thus expanding the role of the DOD in private sector cybersecurity.

CDT has long recognized that there may be a need for a limited exception to the surveillance laws to permit companies to share information to protect other companies and their users. We have called for a targeted, incremental approach that preserves the role of DHS as the locus of civilian cybersecurity efforts, and preserves existing privacy and other protections while creating limited exceptions to facilitate the sharing of carefully defined cybersecurity information.

Though we oppose this bill, we look forward to working toward these goals with both the companies affected by the legislation and members of Congress who will consider it.

Source URL:
https://cdt.org/blogs/greg-nojeim/112cyber-intelligence-bill-threatens-privacy-and-civilian-control

Links:
[1] https://cdt.org/personnel/greg-nojeim
[2] http://cdt.org/blogs/jim-dempsey/dont-mess-success