Version 2.0 of the Senate Intelligence Committee's Cyber Information Sharing Act Is Cyber-Surveillance, Not Cybersecurity

By Robyn Greene, Policy Counsel

Cybersecurity information sharing legislation is like a bad penny – no matter how many times you think you've gotten rid of it, each Congress it keeps popping back up. The notorious Cyber Intelligence Sharing and Protection Act (CISPA, H.R. 234), the primary information sharing legislation in the House of Representatives, has been introduced and re-introduced three times over in the last three sessions of Congress (the Administration issued two veto threats in advance of both House votes so far), and now the Cybersecurity Information Sharing Act (CISA), which raised significant concerns when it originated last year in the Senate Select Committee on Intelligence (SSCI), is expected to be introduced for the second time in early March. The version of CISA that SSCI is expected to consider leaked online.

Despite increasing doubts about whether information-sharing legislation could have prevented an Anthem, Sony, or Home Depot-style hack, CISA's proponents insist that passing cybersecurity information sharing legislation is the single most important way to enhance cybersecurity. However, the bill's primary effect will be to increase cyber-*surveillance*.

As this analysis will explain, the newest version of CISA will not just increase the sharing of impersonal technical data that indicates a cyber threat but will also significantly increase the National Security Agency's access – in fact, all of government's access – to Americans' personal information. It will also allow any entity of the federal government, including intelligence agencies and law enforcement, to use that information for a broad array of garden-variety investigations and prosecutions, not just for cybercrimes. Moreover, CISA would provide a blanket authorization for companies to monitor their users' activities for purposes other than protecting their own networks, as they are currently allowed to do. It also provides companies with complete liability protection for information sharing and monitoring pursuant to the Act. And, to top it all off, CISA has a few worrisome bells and whistles that have nothing to do with information sharing at all, like an authorization for private entities to act as cyber-vigilantes and engage in dangerous countermeasures, and some out-of-place language that has worrisome implications for the NSA's development and use of cyberweapons.

What follows is our best attempt to highlight the most glaring problems with the CISA bill—and propose solutions.

Problem #1: CISA authorizes excessive information sharing, including unnecessary sharing of personal information.

First, the definition of the term "cybersecurity threat" is very broad, allowing companies to share a wide variety of information with the government if there is the mere possibility that there may be "an unauthorized effort to adversely impact" an information system, or information stored on or transiting that system. Before sharing their users' information with the government, a company should at least be required to make a determination that the purported cyber threat is likely to cause harm. (Sec. 2(6))

Additionally, CISA authorizes companies to share an excessive amount of their users' information with the government and with one another. It defines what can be shared, "cyber threat indicators," to include "information that is necessary to describe or identify" any "attribute of a cybersecurity threat" so long as its disclosure is not otherwise legally prohibited. Something that "describe[s]" an "attribute" of a "threat" could be interpreted so broadly as to include personally identifiable information (PII) or the content of private online communications, that is not actually needed to detect or protect against that threat. (Sec. 2(7))

Further, CISA fails to protect users' PII. CISA merely requires that companies remove personal information if the company "knows" that it is not "directly related" to the threat. This weak protection could result in companies unnecessarily sharing the PII of victims, and even their contacts, with the Department of Homeland Security and other companies. Additionally, the "knowledge" requirement allows companies to default to leaving PII in the indicators they share, since they may not know with absolute certainty that the PII they have identified is not directly related to the threat. Instead, CISA should require companies to remove PII from indicators unless it is necessary to identify or mitigate a threat. The bill should also require that government entities review indicators for improperly shared PII, and remove it before using or disseminating the indicators. (Sec. 4(d)(2))

Solution #1: CISA should only authorize a company to share information, including PII, if it is necessary to identify, block or mitigate the impact of a cyber-attack or vulnerability that the company has determined to be likely to cause harm. Additionally, government entities receiving that information should be required to review it for improperly shared PII and remove that PII before disseminating the information further.

Problem 2: CISA Requires DHS to automatically and indiscriminately disseminate to the NSA all indicators it receives.

While CISA only authorizes companies to share threat indicators with DHS, it also requires that DHS immediately disseminate every threat indicator it receives, including all of the personal information that comes with them, to a myriad of government agencies ranging from the NSA to the Federal Bureau of Investigation (FBI) to the Department of Commerce. Management of and response to domestic cybersecurity threats should be controlled by a civilian agency. Requiring a civilian agency like DHS to automatically and indiscriminately disseminate that information to military intelligence agencies like the NSA undermines civilian control. The NSA should only have access to information concerning significant cyber threats, such as threats that could result in a significant loss of life or physical destruction of critical infrastructure; state sponsored espionage, including economic espionage; or the activities of foreign criminal organizations. (Sec. 4(b)(2))

Solution #2: CISA-derived information should only be disseminated to the NSA to address a discrete set of significant threats to national security.

Problem #3: Law enforcement agencies are authorized to use CISA-derived information to investigate a wide array of garden-variety crimes.

If excessive sharing of Americans' personal information is not enough to establish that CISA is as much a surveillance bill as it is a cybersecurity bill, the breadth of investigations and prosecutions that law enforcement can use the information for leaves no room for doubt. It is reasonable to authorize federal and state law enforcement to use CISA-derived cyber threat indicators to investigate and prosecute a clearly defined set of computer crimes. However, CISA authorizes this and much, much more.

CISA allows any entity within the federal government, including intelligence agencies and law enforcement to use the information it receives from companies for investigations and prosecutions into terrorism, which as we've seen over the last year and a half of NSA leaks, is interpreted by the Intelligence Community to constitute a blank check for surveillance of all Americans. It also authorizes entities like law enforcement agencies to use that information in regard to any crimes that could result in imminent death or serious bodily harm, meaning this "cybersecurity" bill would also facilitate investigations into garden-variety violent crimes that have nothing to do with cyber threats. If that weren't worrisome enough, the bill would also let law enforcement and other government agencies use information it receives to investigate, without a requirement for imminence or any connection to computer crime, even more crimes like carjacking, robbery, possession or use of firearms, ID fraud, and espionage. And that's just a few of the crimes on the very long list of crimes for which CISA-derived information can be used.

While some of these are terrible crimes, and law enforcement should take reasonable steps to investigate them, they should not do so with information that was shared under the guise of enhancing cybersecurity. This authorization would not just seriously undermine Americans' Fourth Amendment rights, which would otherwise require the

government to obtain a warrant based on probable cause to access much of that same information, it would create an expansive new means of general-purpose government surveillance. (Sec. 5(d)(5))

Solution #3: Law enforcement entities like the FBI should only be able to use CISA-derived information to investigate or prosecute a clearly defined set of computer crimes. Any authorization for use in investigating violent crimes should be limited to cases where violence is imminent.

Problem #4: CISA authorizes companies to monitor all of their users' activities and communications.

CISA's monitoring provision is unnecessary, overbroad, and would threaten Americans' privacy and Internet security. The federal Electronic Communications Privacy Act (ECPA) protects Internet users' privacy and Internet security by only authorizing companies to monitor their users' activities as necessary to protect their own systems from threats. CISA would undermine those reasonable limitations by providing a blanket authorization for companies to generally monitor their networks for any cybersecurity purpose. (Sec. 4(a))

This would significantly increase the scope of how companies can monitor their customers' online communications and activities. For example, an Internet Service Provider (ISP) that is currently authorized by federal law to monitor traffic on its network in order to identify and counter threats to its own systems would be authorized under CISA to monitor *all* traffic looking for *any* threat to *any* system. That would make everyone a target for monitoring, not just suspicious actors threatening the ISP's network. This authorization could also undermine Internet security because in order to facilitate monitoring, that ISP could attempt to decrypt encrypted communications, or even block encrypted communications from its network.

Solution #4: CISA should not create any new authorization for monitoring, as adequate authorizations already exist in the law.

Problem #5: CISA's liability protections leave customers no recourse if they are wrongly harmed by information-sharing and monitoring.

CISA absolves companies of any liability associated with sharing or monitoring of information pursuant to the Act, except for actions that constitute gross negligence. This provision would preclude causes of action for violations of the Computer Fraud and Abuse Act as well as privacy statutes such as the Stored Communications Act and Wiretap Act portions of ECPA. (Sec. 6)

Solution #5: CISA's liability protections should be narrowed to ensure that there is reasonable recourse for those harmed in the event that a company unnecessarily monitors or shares their personal information.

Problem #6: CISA authorizes companies to deploy dangerous countermeasures and has concerning language regarding military cyber operations.

Lastly, CISA includes provisions that have nothing to do with information sharing at all. It authorizes companies to retaliate against perceived attackers by deploying countermeasures on their systems, like software that would automatically "hack back" against attackers or attempt to retrieve or destroy information that was stolen. While it requires that the countermeasures be deployed only on the company's own network, countermeasures may still unintentionally have extra-network effects, and those extra-network effects could easily include damage to the computers of innocent people whose systems have also been compromised by the attackers. CISA's only other constraint on countermeasures is a weak requirement that the company not intend for the countermeasure to have a harmful or destructive effect on someone else. But if those countermeasures do have such an effect, the company that deployed them would still have been acting pursuant to CISA's authorization. (Sec. 4(c)(1))

Countermeasures are unpredictable and can be difficult to control, and can also fall into the hands of bad actors, all of which increases the risk of unintentional harm to innocent bystanders or victims of botnets or other malicious attacks. And yet if a company deploys a countermeasure on its network that unintentionally harms or destroys the computer systems of a hospital, a Fortune 500 business, a power plant, a friendly foreign government or any other innocent entity, that company would still have been acting within CISA's broad authorization. Cybersecurity information sharing legislation should not include an authorization for the use of such offensive countermeasures, no matter how narrowly drafted, as any such authorization threatens to undermine rather than enhance Internet security.

Finally, CISA also includes an odd rule of construction that states that nothing in the Act should be interpreted to limit the authority of the Secretary of Defense to "develop, prepare, coordinate, or, when directed by the President, conduct military cyber operations." It is unclear why such a statement concerning the Secretary of Defense's authority is needed, or what its intended effect is. What is clear is that the NSA engages in a wide array of offensive cyber activities from purchasing and stockpiling vulnerabilities, to inserting vulnerabilities into software and firmware, to undermining encryption standards, to deploying surveillance malware and even cyberweapons like Stuxnet. Some of these activities may be reasonable; many are certainly not. Regardless, they unquestionably impact the security and functionality of the Internet and the broader computing environment, and their efficacy and legality should be the subject of public debate rather than the subject of vague carve-outs in overbroad cybersecurity information sharing bills. (Sec. 8(m))

Solution #6: CISA should not authorize the use of any offensive countermeasures, and it should not include a Rule of Construction concerning military cyber operations where the necessity and intent of that rule is unclear.

If CISA is intended to increase cybersecurity and not surveillance, it should exclude unnecessarily and dangerously broad authorizations for new monitoring and countermeasures, and it must narrowly define what information can be shared (including robust requirements to remove unnecessary personal information), when information can be shared, and how information can be used. Unless all of the problems we've summarized above are addressed, CISA will do much more to enhance the government's cyber-*surveillance* than it will do to enhance everyone's cybersecurity, and should be strongly opposed.