The Protecting Cyber Networks Act
Undermines Privacy, Enables Cyber-Surveillance, and Threatens Internet Security

By Robyn Greene, Policy Counsel

This month, the House of Representatives is expected to vote on a cybersecurity information sharing bill that unnecessarily and seriously undermines Americans' privacy, and may even undermine cybersecurity itself: the Protecting Cyber Networks Act (H.R. 1560).

PCNA is built off of the framework of the Senate's Cybersecurity Information Sharing Act (CISA, originally introduced in the 113th Congress as S. 2588, and reintroduced this year as S. 754). Both iterations of CISA have raised serious concerns regarding privacy and Internet security amongst privacy advocates and security experts alike, and OTI strongly opposed each version (2014 bill analysis available here; 2015 bill analysis available here).

The House of Representatives' previous cybersecurity information sharing framework, the Cyber Intelligence Sharing and Protection Act (CISPA, currently H.R. 234, H.R. 624 in the 113th Congress, and H.R. 3523 in the 112th Congress) stalled in the face of the same strong opposition from privacy and advocacy groups. The Administration also strongly opposed those bills, threatening to veto them twice, and cautioning that they lacked "clear legal protections and independent oversight," and would "undermine the public's trust in the Government as well as in the Internet by undermining fundamental privacy, confidentiality, civil liberties, and consumer protections." Further, they failed to adhere to three overarching priorities: "(1) carefully safeguard privacy and civil liberties; (2) preserve the long-standing, respective roles and missions of civilian and intelligence agencies; and (3) provide for appropriate sharing with targeted liability protections."

The Protecting Cyber Networks Act (PCNA), like its Senate counterpart, CISA, fails to address these same primary concerns. Specifically, PCNA's most troubling provisions include:

1. Overbroad authorization for monitoring of private Internet communications;
2. Authorization for excessive sharing of sensitive and private information by private companies with the government, including the sharing of unnecessary personally identifiable information (PII);
3. A requirement that any federal entity that receives information under the law immediately disseminate it to the National Security Agency (NSA);

4. Overbroad authorization for government use of information beyond the purpose of improving cybersecurity or prosecuting cybersecurity-related crimes;
5. Authorization for companies to deploy vaguely-defined defensive measures that could harm the computer systems of innocent third parties; and
6. Dangerously broad protection from liability for harms resulting from negligent monitoring, information sharing, or defensive measures.

PROBLEM #1: PCNA would authorize companies to monitor all of their users' activities and communications.

Currently, the Electronic Communications Privacy Act (ECPA) authorizes companies to monitor their networks for self-defense.[1] This means that Internet service providers (ISP) like Verizon, tech companies like Google, banking companies like JP Morgan, retailers like Home Depot and Target, and even entertainment companies like Sony already have all the authority they need to monitor their own systems in order to detect or defend against an attack, without having to get the consent of the individuals communicating over those systems. On the other hand, monitoring for other purposes typically does require the consent of at least one of the parties to each of the communications that is being monitored.

PCNA would completely undermine this privacy protection by providing a blanket authorization for companies to monitor their networks for "cybersecurity purposes". (Sec. 3(a)) This could significantly increase the scope of how companies monitor their customers' or users' online communications and activities. For example, an ISP that can currently monitor traffic in order to identify and counter threats to its own systems would be authorized under PCNA to monitor all traffic looking for any threat to any system. This would mean that everyone would become a target for monitoring, not just suspicious actors threatening the ISP's network. Such a broad allowance for monitoring of private communications is unnecessary and would threaten Americans' privacy.

SOLUTION #1: PCNA should not create any new authorization for monitoring Americans' private communications, as adequate authorizations already exist in the law.

PROBLEM #2: PCNA would authorize excessive information sharing, including the sharing of personally identifiable information that isn't necessary to counter a cybersecurity threat.

In addition to increasing scrutiny of Internet users' activities with expanded monitoring authority, PCNA would also authorize companies to share an excessive amount of their users' information with the government and with one another. (Sec. 4(c)) The bill defines what can be shared, "cyber threat indicators," as some reasonable enumerated indicators of threats such as vulnerabilities and methods of gaining malicious command and control. However, it also

[1] Electronic Communications Privacy Act, 18 USC § 2511 (2)(a)(i).

includes "information that is necessary to describe or identify" any "attribute of a cybersecurity threat" so long as disclosure of the underlying attribute is not otherwise legally prohibited. (Sec. 11(5)) Something that "describe[s]" an "attribute" of a "threat" could be interpreted so broadly as to include PII or the content of private online communications, even when it is not actually needed to detect or protect against that threat. For example, in the case of an ISP customer whose computer has been compromised and is now being used to disseminate phishing spam, the ISP may consider itself authorized to share not only the IP address of that customer, but also the otherwise private identity of the customer to whom the IP address was assigned, and information about the private Internet activity of that customer.

PCNA also fails to adequately protect users' PII. It would require that companies make reasonable efforts to remove PII if they reasonably believe at the time of sharing that it is not directly related to a cyber threat. (Sec. 3(d)(2)) While this requirement is stronger than that in CISA, it would still allow companies to share personal information even if it is unnecessary, so long as it is related to a threat.

SOLUTION #2: PCNA 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.

PROBLEM #3: PCNA would require any federal entity that receives cyber threat indicators to automatically and indiscriminately disseminate them to the NSA and other federal agencies.

Not only would PCNA authorize excessive information sharing from businesses to government, it would also authorize excessive sharing of that same information throughout the government, while also undermining civilian control of domestic cybersecurity information sharing. While PCNA would only allow companies to share information directly with a civilian federal entity (Sec. 3(c)(1)(A)), it would also require any civilian entity that receives indicators to immediately disseminate all threat indicators they receive, including personal information, to a myriad of government agencies ranging from the NSA and the Office of the Director of National Intelligence to the Federal Bureau of Investigation (FBI) and the Department of Commerce. (Sec. 4(a)(B), newly created section "(b)(2)(i))") It would also prohibit those civilian entities from doing anything to impede the real-time dissemination of indicators, or to modify them in any way. (Sec. 4(a)(B), newly created section "(b)(2)(ii))") This would make it impossible for the original receiving entity to conduct a second review of indicators to identify and remove any improperly shared personal information before transmitting it to the NSA or other agencies.

Management of and response to domestic cybersecurity threats should be controlled by a civilian agency. Requiring a civilian agency to automatically and indiscriminately disseminate that information to military and intelligence agencies like the NSA undermines civilian control. Entities within the Department of Defense, like 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 or state sponsored espionage.

SOLUTION #3: Government entities receiving information under PCNA should be required to review it for improperly shared PII and remove that PII before disseminating the information further, and that information should only be disseminated to the NSA when it concerns significant threats to national security.

PROBLEM #4: PCNA would authorize the government to use shared information for investigations and prosecutions that have nothing to do with cybersecurity or computer crime.

In addition to allowing companies to share personal information that is not necessary to identify or respond to a cybersecurity threat and requiring that the NSA receive all of that information, PCNA would also authorize the federal government to use information they receive in investigations and prosecutions that have nothing to do with cybersecurity or computer crime. This makes PCNA as much a surveillance bill as it is a cybersecurity bill.

PCNA would allow any entity within the federal government, including intelligence agencies and law enforcement, to use the information it receives from companies for investigation or prosecution of any crimes that could result in death or serious bodily harm, without requiring that the harm be imminent or that the crime be computer-related. That means the data shared under this "cybersecurity" bill could be used to investigate garden-variety violent crimes that have nothing to do with cyber threats. This allowance for investigation or prosecution of physical crimes that are unrelated to cybersecurity could be read aggressively to extend to preventing acts of terrorism, which as we've seen over the last year and a half of NSA leaks may be interpreted by the Intelligence Community to constitute a blank check for surveillance of all Americans.

If that weren't worrisome enough, the bill would also let law enforcement and other government agencies use information it receives to investigate, also without a requirement for imminence or any connection to computer crimes, a long list of crimes that includes carjacking, robbery, arson, possession or use of firearms, ID fraud, and espionage.

While some of these are serious crimes, and law enforcement should take reasonable steps to investigate them, they should not do so with information that was shared for the purpose 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, but would create an expansive new means of general-purpose government surveillance. (Sec. 4(d)(5)(A))

SOLUTION #4: Law enforcement entities like the FBI should only be able to use PCNA-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 #5: PCNA would authorize companies to deploy defensive measures that may cause unintended harm to innocent bystanders.

PCNA would not only threaten privacy, it could also threaten Internet security. PCNA would authorize companies, notwithstanding any other provision of law—including anti-hacking statutes like the Computer Fraud and Abuse Act—to deploy defensive measures on their networks against perceived attackers. This authorization is not only unnecessary but so broad and ambiguous that it could allow companies to deploy measures that may unintentionally harm or destroy a third party's system.

The authorization would permit companies to deploy defensive measures on their systems, but it includes an important restriction that the effects of those defensive measures must be limited to one's own system, or another entity's system pursuant to their consent. (Sec. 3(b)(1)) However, this restriction is subject to a limitation which states that a defensive measure may not intentionally or recklessly "destroy[], render[] unusable or inaccessible (in whole or in part), substantially harm[], or initiate[] a new action, process, or procedure on [another entity's] information system or information stored on, processed by, or transiting [another entity's] information system." (Sec. 3(b)(2))

This limitation creates ambiguity because on the one hand, the authorization states that the effects of a defensive measure must be limited to one's own system, but on the other hand, it states that defensive measure cannot intentionally have destructive effects. Thus the limitation suggests that a defensive measure may have unintentional extra-network effects. If that is the case, PCNA might authorize a company to operate a defensive measure that unintentionally causes damage, destruction, or substantial harm to another entity's information system, or that unintentionally initiates a new action, process, or procedure on another entity's information system or information stored on, processed by, or transiting another entity's information system. And that company would be immunized against liability for that damage—even if the damage was the result of negligence—so long as the company's conduct was not "reckless".

Further, it is unclear what level of harm must occur to constitute "substantial harm." This is a particularly important question considering that PCNA would apparently authorize a company to deploy a defensive measure in a manner that caused harm to an innocent third party's systems, so long as that harm was not determined to be substantial. Even if the harm was to the computer systems of a hospital, a Fortune 500 business, a power plant, a friendly foreign government or any other innocent entity or individual, that company would still have been acting within PCNA's authorization and would be protected against liability for that harm.

In addition to the concern about what harms may result from the authorization to deploy defensive measures, the need for this new authorization is unclear. Under current law, entities can take actions on their own networks to defend those networks. For example, they can employ firewalls, block known malicious IP addresses from accessing their networks with DNS blacklists, allow only authorized users access to their networks with DNS white lists, scan traffic on their networks to identify malicious code, and set up fake targets or "honeypots" on their networks to lure attackers away from sensitive information and gain information about them that

is needed to defend those networks. With such a range of options already available, a new authorization to use broadly defined "defensive measures" carries great risk for little reward.

SOLUTION #5: PCNA should not create any new authorization to use defensive measures.

PROBLEM #6: PCNA would immunize companies from liability for harms resulting from information sharing and monitoring.

PCNA would also absolve companies of any liability associated with information sharing or monitoring conducted pursuant to the Act, except for actions that constitute willful misconduct that the harmed party must establish with a high burden of evidentiary proof. 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) Information sharing and monitoring that negligently or even recklessly violated the law would be immunized by PCNA, regardless of how substantial is the damage to other computer systems, individuals' privacy rights, or any other legal interest.

SOLUTION #6: PCNA'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.

Conclusion

For nearly two years, Americans and people the world over have learned of the NSA's near-ubiquitous surveillance abilities and practices. Now more than ever before, Congress should ensure that strong privacy protections are central to the provisions of any cyber information sharing legislation that it passes.

At a minimum, cybersecurity information sharing legislation must provide for effective civilian control of information sharing between the private sector and the government while placing meaningful limits on the role of military and intelligence agencies like the NSA. That legislation also must include strong privacy protections to shield innocent Americans' sensitive information, including limiting its use to investigations and prosecutions of computer crimes; narrowly tailored liability protections to ensure that parties who are negligently harmed may seek redress for those harms; and no new authorizations for additional monitoring of private communications nor for the deployment of countermeasures.

PCNA, like CISA, fails on all of these counts. It would enhance cyber-surveillance while threatening to undermine cybersecurity.