The Heritage Foundation

ISSUE BRIEF

No. 4382 | APRIL 10, 2015

House Cyber Information Sharing Bills: Right Approach but Require Fixes

David Inserra and Riley Walters

In March, the House of Representatives released several pieces of legislation on the sharing of cyber information. Two of the more noteworthy of these bills are: H.R. 1560, Protecting Cyber Networks Act (PCNA), introduced by Representatives Devin Nunes (R–CA) and Adam Schiff (D–CA) in the House Intelligence Committee, and the National Cybersecurity Protection Advancement Act (NCPAA) of 2015, introduced by Representative Mike McCaul (R–TX) in the House Homeland Security Committee. According to press reports, these bills are not competitors but rather complementary efforts.[1]

Information sharing is a basic way to improve cybersecurity by enabling companies and the government to share information on current cyber threats and vulnerabilities. With more information sharing, both the government and the private sector can be better prepared to stop or mitigate cyber risks. Though these bills are on the right track, neither correctly handles the three most salient details: strong liability protection, broad ability to use shared information, and robust but not redundant or burdensome privacy measures. It is also important to note that information sharing will not stop all threats; such bills are just the first step toward improving U.S. cybersecurity.

This paper, in its entirety, can be found at **http://report.heritage.org/ib4382**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Liability Protection

Both cyber bills have common language not authorizing additional surveillance measures, not changing past sharing agreements, forbidding use by federal agencies for regulatory purpose or tying of grant funding to information sharing, prohibiting anti-competitive behavior, and protecting from Freedom of Information Act (FOIA) requests. They diverge, however, on liability protection for sharers. For non-federal entities that do share information, a strong liability protection is necessary.[2]

On this point, the NCPAA bill's verbiage is stronger than the PCNA bill. The NCPAA states that a "non-Federal entity...shall not be liable in any civil or criminal action brought under this subsection unless such non-Federal entity engaged in willful misconduct or gross negligence with respect to such sharing or conduct and such gross negligence or willful misconduct proximately caused injury."[3] This standard of willful misconduct or gross negligence is strong language that will protect companies that share information and better incentivize rapid sharing of cyber information.

The PCNA states that "no cause of action shall lie or be maintained in any court against any non-Federal entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure if such sharing or receipt is conducted in good faith."[4] While "good faith" is an attempt to protect sound information sharing, it is a lower standard of proof that is more easily challenged by tort lawyers, opening companies up to greater risk of litigation. While the PCNA does mention willful misconduct, the good faith standard posited just a subsection earlier would be likely to trump it.

Privacy Measures

When it comes to cyber information sharing, the types of information that are being shared include the coding of a virus, the route an attacker used, or a hole in security. However, there may be some personal information attached that is not relevant to dealing with cyber threats, indicators, defensive measures, or risks. While security professionals have no interest in this information, there is a trade-off between removing all unnecessary information and sharing information in a timely manner.[5]

Both bills require that "reasonable" measures be taken to remove any personal information that is unrelated to a cyber risk or incident before sharing with the federal government or other non-federal entities.[6] The PCNA also provides non-federal entities the ability to take reasonable efforts to "implement a technical capability configured to remove any [personal] information." This technical capability is a possible nod toward the Structured Threat Information eXpression (STIX) standardized language and mechanisms for sharing information that enable sharers to limit what proprietary or private information is shared without slowing information sharing.[7]

The PCNA and the NCPAA also establish a series of other privacy guidelines and reports. The PCNA charges the Attorney General, the Privacy and Civil Liberties Oversight Board (PCLOB), the Director of National Intelligence (DNI), and inspectors general (IGs) with this responsibility while the NCPAA charges the Department of Homeland Security (DHS) Under Secretary for Cybersecurity and Infrastructure Protection, the DHS Chief Privacy Officer, IGs, and the PCLOB. [8]

While some reports on privacy are certainly important and necessary, both bills seem to create too many reporting requirements and should be streamlined to ensure that duplicative tasks are not being asked of multiple privacy and oversight organizations. Both bills also include provisions that properly punish government workers who wrongfully use information, limit the use and retention of information containing personal data, and notify private-sector sharers when they are sharing information improperly.

Government Sharing and Use of Information

When sharing with the federal government, the NCPAA empowers the DHS's National Cybersecurity and Communications Integration Center (NCCIC) to act as the primary hub for public-sector and private-sector information, though other information-sharing arrangements can and should continue. While DHS is the appropriate spot for such a hub, DHS capabilities have been questioned, though progress is being made.[9]

The PCNA, on the other hand, does not designate a hub but allows the President to establish the government hub or hubs that the private sector can share with, including the Departments of Commerce, Energy, Homeland Security, Justice, Treasury, or the DNI, but explicitly rejecting direct

1. Cory Bennett, "Advancing Cyber Bills Spark Fresh NSA Worries," *The Hill*, April 3, 2015, http://thehill.com/policy/cybersecurity/237758-advancing-cyber-bills-spark-fresh-nsa-worries (accessed April 8, 2015).
2. David Inserra and Paul Rosenzweig, "Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2899, April 1, 2014, http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace.
3. National Cybersecurity Protection Advancement Act of 2015, 114th Cong., 1st Sess., http://www.scribd.com/doc/259428604/National-Cybersecurity-Protection-Advancement-Act-Draft-3-20-15 (accessed April 9, 2015).
4. Amendment to Protecting Cyber Networks Act, H.R. 1560, 114th Cong., 1st Sess., http://docs.house.gov/meetings/IG/IG00/20150326/103265/BILLS-114-HR1560-N000181-Amdt-1.pdf (accessed April 9, 2015), and Protecting Cyber Networks Act, H.R. 1560, 114th Cong., 1st Sess., http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/ProtectingCyberNetworksbilltext.pdf (accessed April 9, 2015).
5. Inserra and Rosenzweig, "Cybersecurity Information Sharing."
6. Amendment to Protecting Cyber Networks Act, H.R. 1560; Protecting Cyber Networks Act, H.R. 1560; and National Cybersecurity Protection Advancement Act of 2015.
7. Inserra and Rosenzweig, "Cybersecurity Information Sharing."
8. Amendment to Protecting Cyber Networks Act, H.R. 1560; Protecting Cyber Networks Act, H.R. 1560; and National Cybersecurity Protection Advancement Act of 2015.
9. National Cybersecurity Protection Advancement Act of 2015.

information sharing with the Department of Defense (DOD).[10] The hub or hubs would then share information among themselves and with the DOD, as well as other federal departments as necessary. To oversee this system, the PCNA empowers the newly created Cyber Threat Intelligence Integration Center to ensure that sharing is occurring and then to analyze intelligence to inform the President, relevant departments, and Congress.

Once correctly shared information is in government hands, it should be broadly useable. While this information will primarily be used for a cybersecurity purpose, legally and voluntarily shared cybersecurity information could also have implications for national security, public safety, or business or individual financial and identity security. Since the data that is shared is not focused on the content of e-mails or personal information, the government should be allowed to use cyber threat data for other purposes as well.[11]

The PCNA lists a series of authorized uses including cybersecurity, preventing death or serious bodily harm, preventing the exploitation of minors, preventing and prosecuting violent felonies, fraud and identity theft, and espionage and the theft of trade secrets.[12] The NCPAA, on the other hand, allows shared information to be used "solely for cybersecurity purposes."[13] The PCNA's standard is not perfect, but it is sufficiently broad to be helpful in acting against other serious crimes, while the NCPAA standard is wholly deficient.

Steps for Congress

As shown above, both the PCNA and the NCPAA have strong and weak provisions. According to press reports, these bills are designed to be complementary, i.e., their differences will be resolved and they will either be combined or otherwise coordinated and connected.[14] Little information, however, is publically available regarding how these two bills will mesh, especially given that each has a different liability system, different sharing hub, and different authorized uses for shared information.

Regardless, whatever comes out of the House should provide a clear system of rules by which public and private entities can share information. Congress should:

- **Streamline privacy provisions.** Privacy provisions that overly impede information sharing should be revised. The adoption of STIX or other automated systems of scrubbing personal data and sharing information should be encouraged. Duplicative privacy provisions and reporting requirements should be streamlined.

- **Provide strong liability protection**. By providing strong liability protection for information that is shared, businesses will be encouraged to share with the government as well as with other businesses. The NCPAA provides a strong standard except in cases of willful misconduct or gross negligence, while the PCNA provides a murkier "good faith" protection. To better enable information sharing, sharers should be protected as long as they do not commit willful misconduct or gross negligence.

- **Broaden authorized uses of shared information.** While the PCNA allows the government to use information for a somewhat broad list of purposes, the NCPAA restricts government use to just cybersecurity purposes. Congress should broaden the government's use of properly shared information, allowing its use so long as one significant use is for a cybersecurity purpose.

Securing Information Sharing

Both information sharing bills have positive and negative elements. The PCNA has relatively weak liability protection for sharers and some redundant privacy requirements while having a good list of authorized uses. The NCPAA has strong liability protection but severely restricts the government's use of shared information and has some duplicative

10. Amendment to Protecting Cyber Networks Act, H.R. 1560; Protecting Cyber Networks Act, H.R. 1560; and Cory Bennett, "House Intel Unveils Cyber Sharing Legislation," *The Hill*, March 24, 2015, http://thehill.com/policy/cybersecurity/236752-house-intel-panel-unveils-final-piece-of-cyber-puzzle (accessed April 8, 2015).
11. Inserra and Rosenzweig, "Cybersecurity Information Sharing."
12. Amendment to Protecting Cyber Networks Act, H.R. 1560, and Protecting Cyber Networks Act, H.R. 1560.
13. National Cybersecurity Protection Advancement Act of 2015.
14. Bennett, "Advancing Cyber Bills Spark Fresh NSA Worries."

reporting provisions. Both could be improved by drawing on the other's strengths and ensuring that information sharing is more strongly encouraged and that the shared information is used as effectively as possible.

*—**David Inserra** is a Research Associate for Homeland Security and Cyber Security in the Douglas and Sarah Allison Center for Foreign and National Security Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation. **Riley Walters** is a Research Assistant in the Allison Center.*