The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3594 | MAY 8, 2012

CISPA Disappoints in the End

Paul Rosenzweig

As the House began its consideration of cybersecurity legislation last month, there was reason to be optimistic about the course that the House Leadership and the House Intelligence Committee had set. The Cyber Intelligence Sharing and Protection Act (CISPA), as it went to the floor, was imperfect to be sure, but it had many virtues: simplicity of conception, ease of understanding, and, most importantly, an intent to incentivize and energize the sharing of critical cybersecurity threat and vulnerability information between the private sector and the government.

The bill that passed the House last week differs from the one that went to the floor. And while the effort remains a laudable one, it must in candor be said that the end product of House deliberations is disappointing when compared to the bill as originally proposed. Three changes in particular were mistakes that should not find their way into any final bill.

Use/Purpose Limitation. When passed out of committee and sent to the floor, CISPA contained a broad provision that authorized private-sector cybersecurity threat and vulnerability information that had been shared with the federal government to be distributed widely in the government, as long as "one significant purpose" of the distribution was either a cybersecurity or national security purpose. This language was a mirror of the successful language used in the Patriot Act to tear down walls and silos of information that had prevented American security agencies from connecting the dots of 9/11. In effect, it meant that as long as a significant reason for sharing was a cybersecurity or national security reason, the information that was shared could be used for any lawful purpose—for example, to identify narcotics cartels.

As passed by the House, however, cyberthreat and vulnerability information shared with the federal government may now be used only for one of five specific purposes: a cybersecurity purpose; to investigate a cybercrime; for a national security purpose; to protect individuals from the danger of death or serious bodily injury; or for the protection of minors from child pornography or sexual exploitation.

This is a deeply problematic change in the law. It is a step back toward the ill-conceived stovepipe system of information collection and dissemination that led to many of the flaws identified by the 9/11 Commission. It would require, in the first instance, a huge bureaucratic structure to monitor compliance and it would, as this type of structure did before 9/11, make those who would share information overly cautious. The U.S. intelligence community has spent the past 10 years trying to break down walls and move from a "need to know" culture to a "need to share" culture. These limitations are a severe step backward and would only recreate turf wars and artificial distinctions that could endanger lives, property, and the best interests of American security.

A further consequence of this re-erection of walls is that the drafters had to decide which federal interests fell on which sides of the wall. What crimes would have the same federal importance as national security, and be acceptable grounds for sharing

This paper, in its entirety, can be found at **http://report.heritage.org/ib3594**

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies

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

cyberthreat information? Looking at the list, one wonders, for example, who would defend the proposition that cyberthreat information that incidentally revealed serious economic espionage, multibillion-dollar fraud, or drug dealing should not be shared within the federal government? Yet that is what the law now says.

The wise policy choice—the one that the 9/11 Commission recognized—is that artificial line drawing is just that—artificial. The right way to protect privacy is not to arbitrarily inhibit government action, but rather to insure that government's use of data and information is subject to continuous oversight. It is a serious mistake for any bill to accept the re-imposition of artificial barriers between investigative agencies; doing so admits the possibility of returning to the unfortunate rules that predated the 9/11 attacks and hampered U.S. security.

Liability Protections. No private-sector actor will share cyberthreat or vulnerability information with the government or other private-sector actors if doing so will result in being sued. That means that actors whom the government wants to incentivize to share threat information must be protected from liability in court. Unfortunately, the liability provisions of the bill were substantially weakened during floor consideration.

Previously (as presented to the Rules Committee), the bill had protected private-sector actors against liability unless the sharing entity had engaged in "willful misconduct." That is the appropriate standard that should be utilized when such important interests are at stake and lives may be on the line. Now, the liability provisions protect only entities who acted "in good faith." Since an allegation of "bad faith" is relatively easy to plead with a few imaginative facts that will survive summary dismissal, it opens up American companies to hugely expensive and distracting discovery disputes, executive-level depositions, and civil litigation costs from abusive litigation that may include defense attorney fees even if the corporation has done everything right. In short, the incentives for both ideologically driven lawsuits and trial lawyer strike suits are significantly magnified. Indeed, the new provisions are a tort lawyer's and anti-corporate activist's dream. Faced with this inadequate liability protection, many entities will simply choose not to share vital information, defeating the whole purpose of the bill.

Sunset Provision. The bill now has a sunset provision in it. By its terms, the entire bill is repealed in five years. In context, this sunset provision is inadequate and possibly ambiguous. It is written as a complete repeal of the bill. This has the effect of repealing a liability limitation, which is problematic: Do acts that had been protected from liability (because they were done in accordance with authorization of the act and in good faith) suddenly become actionable, because the underlying authorization has been repealed and the liability limitation as well? It is impossible to tell from the language of the bill, making its likelihood of succeeding in encouraging the sharing of essential information even more doubtful. At a minimum, the sunset provision needs a saving clause of some sort.

Going forward, as a matter of public policy, these critical flaws in the bill need to be fixed. As drafted, it is not at all clear that the legislation is worth the effort.

*—**Paul Rosenzweig** is a Visiting Fellow in the Center for Legal and Judicial Studies and the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*