

General Q&A about the Rogers-Ruppersberger Cybersecurity Bill

Q: What's the status of the Rogers-Ruppersberger cybersecurity bill?

A:

- The bill has been reported out of committee on a bipartisan 17-1 vote and is currently awaiting floor action in the House of Representatives.

Q: Is it too late to offer suggestions or recommendations for the bill?

A:

- Not at all. The key bipartisan sponsors of the legislation have met a number of times with various groups, including key representatives from the business community and privacy and civil liberties groups to address questions and concerns; these meetings will continue as the bill comes to the House floor and we will continue to make any needed changes in the coming days and weeks.
- Indeed, after meeting with a number of privacy and civil liberties groups, the bipartisan cosponsors made two major amendments to the legislation that were accepted by voice vote in committee.
 - First, an amendment proposed by the Chairman and Ranking Member that added significant civil liberties and privacy protections was adopted at committee markup and includes an anti-tasking provision and an anti-quid pro quo provision to prevent any attempt to make this bill a surveillance program, as well as an anti-data mining provision and use limitation to restrict how the government may search and use any data voluntarily provided by the private sector.
 - Second, an amendment offered by Congressman Mike Thompson (D-CA) was adopted at committee and provides for an independent, detailed review of the federal government's use of voluntarily shared information by the Inspector General to be provided to Congress on an annual basis.
- In addition, a number of new changes are being considered for the legislation as it moves to the House floor, including provisions to give a more prominent role to the Department of Homeland Security, permitting lawsuits against the federal government if the government improperly uses information voluntarily provided by the private sector, and provisions to clarify that no new authority is being provided to the Department of Defense or the Intelligence Community to direct or require public or private sector cybersecurity efforts.

Q: I've heard that the bill has no protections for privacy and civil liberties; is that right?

A:

- No. To the contrary, the bill contains strong, customized privacy protections designed to ensure that the bill remains centrally focused on protecting cybersecurity.
- First, the bill is completely voluntary; no one is required to change anything about what they do today as a result of the legislation.
- Second, the bill focuses on cyber threat information sharing, allowing the government to provide classified cyber threat intelligence to the private sector and permitting the private sector to identify and share cyber threat information on a voluntary basis.
- Third, the bill only permits information directly pertaining to threats or vulnerabilities to be identified and shared only for the purpose of protecting systems and networks from such threats or vulnerabilities.
- Fourth, the bill authorizes (and encourages) the private sector to anonymize or minimize the cyber threat information it voluntarily shares with others, including the government.
- Fifth, if the cyber threat information is voluntarily shared with the government, there are strong limitations on the government's use of the information.
 - The cyber threat information must be protected from disclosure outside the federal government unless further sharing is specifically authorized by the entity providing the information.
 - The government may not search the cyber threat information for non-cybersecurity or national security information. (Amendment at markup)
 - The government may not use the cyber threat information for other purposes unless a significant cybersecurity or national security purpose exists. (Amendment at markup)
 - The government may not require any entity to share cyber threat information with the government. (Amendment at markup)
 - The government may not require the sharing of cyber threat information in exchange for government cyber threat intelligence. (Amendment at markup)

- Sixth, if the government violates any of the restrictions placed on it by the legislation, it can be held liable for damages, costs, and attorney's fees through federal lawsuits. (New provision).

Q: Some have said that the bill permits the government to engage in a wide-ranging surveillance program; is that true?

A:

- No. The bill does not permit government surveillance. It allows the government to share classified threat information with the private sector to help the private sector better defend its own networks; the bill also provides clear authority to the private sector—not the government—to identify and share cyber threats on its own systems and networks.
 - The bill only permits such private sector identification and sharing of cybersecurity threat information where a company is engaged in the protection of its own systems or networks or those of a corporate customer; it does not permit the monitoring of individual customers.
- The bill does not require anyone to provide information to the government; any sharing of information with others—whether in the private sector or in government—is completely voluntary.
 - Rather than requiring information to be provided to the government, the bill explicitly bars the government from requiring private companies to provide it information. (Amendment at markup)
 - Moreover, the bill also specifically prohibits the government from offering intelligence only if the private sector provides information back; rather, the government must provide useful intelligence to the private sector regardless of whether it receives any information back from the private sector. (Amendment at markup)
 - Indeed, if the government violates either of these prohibitions—or various other restrictions in the legislation—the bill makes the government liable for damages, costs, and attorney's fees in a federal court action. (New provision)
 - As such, the government's only role under the bill is to provide intelligence information to the private sector to help the private sector to protect itself and to provide assistance if the private sector voluntarily chooses to provide information to the government.

- In addition, the bill specifically permits the private sector to restrict the cyber threat information it shares, including anonymizing or minimizing the data shared with the government.
 - And the bill lets the private sector share as much or as little cyber threat information as it wants and allows the private sector to hold back any sensitive information it deems appropriate.

Q: Some bloggers have said that the definition of “cyber threat information” in the bill is too broad and permits private sector companies to monitor and obtain all manner of information that may be completely unrelated to cybersecurity; is that true?

A:

- No. The definition of “cyber threat information” in the bill is limited only to information that directly pertains to a threat to, or vulnerability of, a system or network.
 - This definition ensures that the only information being identified or shared is limited to information about real cyber threats and vulnerabilities.
 - Today, the Chinese and other nation-state actors are stealing reams upon reams of corporate information and sensitive government information right out from under our noses; this expansive, aggressive effort undermines the free market and costs valuable American jobs. We must provide our private sector the information it needs to defend itself.
 - Similarly, hackers are out there stealing tremendous amounts of personal information belonging to individuals, from credit card and social security numbers to medical records. We must provide the companies that provide critical services to ordinary Americans with the threat information they need to protect our personal information.
 - We continue to work with various groups to see if the definitions in the legislation can be even more narrowly tailored, but it is important that any definitions be flexible enough to deal with rapidly changing technologies and the various adaptive tactics used by high-end nation-state hackers.
 - The law is hard to change and locking in technology-based definitions can lead to significant challenges.

- It is also important to ensure that any definitions in the law not provide a roadmap for attackers to determine exactly what types of threats can be identified and then develop techniques that aren't covered by the law.
- It is also important to note that under the bill a company may only identify and share cyber threat information for “cybersecurity purposes”; that is only when they are seeking to protect their own systems or networks or those of their corporate customers.
 - This means that the bill only authorizes activities when companies are actually protecting themselves or their corporate customers against real threats to their systems or networks.
- The combination of these provisions helps ensure that privacy and civil liberties will properly be protected.

Q: Some have argued that this bill puts the military or the intelligence community in charge of cybersecurity; is that correct?

A:

- The bill only permits the Director of National Intelligence to create procedures and guidelines for the sharing of cyber threat intelligence from the government to the private sector and for the granting of security clearances for cybersecurity purposes; the intelligence community has no other role under the legislation.
- The bill would require the Department of Homeland Security to generally receive copies of all voluntarily shared cyber threat information for the purpose of ensuring that the information was shared for cybersecurity purposes. (New provision)
- The Department of Homeland Security would also generally have the role of sharing voluntarily shared information within the government and would be required to be consulted on the Director of National Intelligence's sharing and security clearance procedures and guidelines. (New provision)
- The bill would also make clear that it grants no new authority to the Department of Defense or the Intelligence Community to require or direct any private or public cybersecurity efforts. (New provision)

Q: Some have said that the bill should limit the government's use of voluntarily shared information to cybersecurity purposes or the prosecution of cybersecurity crimes; would this be a good idea?

FACT:

- No. Limiting the government's use of voluntarily shared information to a handful of specific purposes runs the risk of the government having to ignore information that it has in its possession.
 - For example, if the government was restricted to only using the information shared for cybersecurity purposes, the government might be required to ignore information properly provided to the government, even if it described a terrorist plot or contained specific evidence of child pornography being created.
- The bipartisan sponsors of the legislation believe it is critically important, however, to ensure that the government only obtains the information for cybersecurity purposes and only uses it for other purposes when it already has a legitimate (and significant) cybersecurity or national security purpose.
 - As a result, the bill only allows the government to use voluntarily shared information for non-cybersecurity or national security purposes when it also has a separate, significant cybersecurity or national security purpose. (Amendment at markup)
 - So, for example, the government could only use voluntarily shared information constituting evidence of child pornography to pursue the pornographer if the government properly received the information for cybersecurity purposes and had a cybersecurity or national security use for the information.
 - And, if the government violates this use limitation, the bill provides for government liability for actual damages, costs, and attorney's fees in a federal court lawsuit. (New provision)
- These provisions together ensure that information cannot be shared with the government or used under this bill unless there is a direct tie to cybersecurity.
 - This is more protective than even the Administration's proposal and some of the bills in the Senate that would generally permit broad law enforcement use of shared cyber threat information.

Q: Doesn't this bill—like other controversial pieces of legislation previously considered by Congress—allow the government to manipulate Internet transactions or shut down websites?

FACT:

- Unlike other controversial legislation, nothing in this bill provides any authorities requiring companies to take particular content off the Internet or to stop access to particular websites.
- To the contrary, the bill imposes no requirements whatsoever on individuals or entities using the Internet. The purpose of the bill is to provide the private sector with access to government intelligence information to allow companies to better protect themselves and to allow companies—on a purely voluntary basis—to share information to better protect themselves.
- And if the private sector voluntarily chooses to provide the government with certain cyber threat information, there are strict limitations on the government's ability to use, search, or further share that information. And these limitations are specifically enforced by a government liability provision that holds the government accountable through federal lawsuits. (Amendment at markup and new provision)

Q: How can I be sure that the private sector won't improperly share my information with the federal government?

A:

- First, in order to address privacy and civil liberties concerns, the legislation was designed to focus on the activities of corporate entities, not individuals. As a result, the bill's definitions specifically exclude individuals from being covered by the bill.
- Second, the bill only allows the voluntary sharing of cyber threat information, which is defined only to include information directly pertaining to a threat to, or vulnerability of a system or network. There are no mandates or requirements related to information-sharing in this bill.
- Third, such cyber threat information may only be shared with the federal government for cybersecurity purposes, which is likewise defined to only include the purpose of protecting a system or network from a threat or vulnerability.

- Fourth, the liability limitation provided by the legislation only applies to the activities discussed above, so if a company were to share information that doesn't fit the definition of cyber threat information or to share information for purposes other than cybersecurity, individuals could sue the company.
- Fifth, the bill provides specific restrictions on the government, institutes protections against the misuse of voluntarily shared information, and creates penalties to be levied against the government in federal lawsuits if it violates the bill's provisions.
 - For example, the government may not generally use voluntarily shared information unless it first has at least one significant cybersecurity or national security use. (Amendment at markup)
 - Similarly, the government may not affirmatively search voluntarily shared information for purposes other than national security or cybersecurity. (Amendment at markup)
 - And the government may not require anyone to share information with the government nor may it limit the sharing of intelligence information to companies that voluntarily share information back to the government. (Amendment at markup)
 - All of these restrictions are enforceable against the federal government because the bill makes the government liable for damages to individuals in federal court if it violates any of these provisions. (New provision)

Q: What can I do if I think my information is being misused by the government?

A:

- The bill specifically provides for lawsuits against the federal government if it violates any of the restrictions provided in the bill to protect privacy and civil liberties. (New provision)
- Specifically, the bill provides a cause of action for people if the government fails to abide by the affirmative search restriction, the use limitation, the anti-tasking provision, the anti-quid pro quo provision, and the provision limiting sharing outside the federal government to those approved by the sharing entity, among others, that provide strong, customized protections for civil liberties. (New provision)

- This cause of action would permit plaintiffs to bring a lawsuit in federal court against the government and would permit individuals to collect actual damages, costs, and attorneys fees from the government if the court finds a violation of the statute. (New provision)
- Provisions like this one—making the government liable to pay damages—are typically used to prevent the government misuse of information in a wide range of laws, including the federal Privacy Act.