Minority Views of Senator Ron Wyden

Cyber-attacks and hacking against U.S. companies and networks are a serious and growing problem, with very real consequences for American companies and American consumers, and pose a significant challenge for national security. I share my colleagues' view that Congress should do what it can to help address this problem. The most effective way to protect cybersecurity is to ensure that network owners take responsibility for security and effectively implement good security practices. And it is important to ensure that government agencies do not deliberately weaken security standards.

It also makes sense to encourage private companies to share information about cybersecurity threats. However, this information-sharing must include strong protections for the privacy rights of law-abiding American citizens. Any information-sharing legislation that lacks adequate privacy protections is not simply a cybersecurity bill, but a surveillance bill by another name.

I opposed this bill because I believe its insufficient privacy protections will lead to large amounts of personal information being shared with the government even when that information is not needed for cybersecurity. This could include email content, financial records, and a wide variety of personal information. While corporations will have a choice about whether or not to participate in this sharing, they could do so without the knowledge or consent of their customers, and will be granted immunity from liability if they do so. Additionally, this bill trumps federal privacy laws and permits government agencies to use the collected information for a wide variety of purposes, rather than only to protect cybersecurity. The bill also creates a peculiar double standard, in that personal information about individual consumers can be used for a variety of non-cybersecurity purposes, including law enforcement actions against those consumers, but information about the companies supplying the information generally may not be used to regulate those companies. In my judgment it does not make sense to say that corporations' privacy is more important than individuals' privacy.

This excessively broad collection may not be the intent of this bill, but the language is clearly drafted broadly enough to permit it. Most notably, the bill defines a cybersecurity threat as anything that "may result" in harm to a network. This broad definition will incentivize the sharing of information even when it is unlikely to pertain to an actual cybersecurity threat. A more tailored definition, limited to actions that are reasonably likely to harm or interfere with a network, would ensure that information-sharing was more narrowly focused on actual threats.

A more tailored approach would also specify that companies should only provide the government with individuals' personal information if it is necessary to describe a cybersecurity threat. This would discourage companies from unnecessarily sharing large amounts of their customers' private information. This bill unfortunately takes the opposite approach, and only requires private companies to withhold information that that is known at the time of sharing to be personal information unrelated to cybersecurity. This approach will disincentivize companies from carefully reviewing the information that they share and lead to a much greater amount of personal information being transferred unnecessarily to law enforcement and intelligence agencies.

I am also concerned that this legislation does not provide individuals with an adequate mechanism for redress in cases where the government violates the rules established by this act. Similar bills have included provisions permitting individuals harmed by such violations to recover damages from the government, and in my judgment such a provision is needed in this bill as well.

I am disappointed that the committee did not adopt stronger privacy protections in this legislation, and I am also disappointed that my amendment to prohibit government agencies from requiring U.S. hardware and software companies to build weaknesses into their products was not adopted. I have introduced this amendment as stand-alone legislation and will continue to pursue this goal.

Finally, I remain very concerned that a secret Justice Department opinion that is of clear relevance to this debate continues to be withheld from the public. This opinion, which interprets common commercial service agreements, is inconsistent with the public's understanding of the law, and I believe it will be difficult for Congress to have a fully informed debate on cybersecurity legislation if it does not understand how these agreements have been interpreted by the Executive Branch.

I have repeatedly asked the Department of Justice to withdraw this opinion, and to release it to the public so that anyone who is a party to one of these agreements can consider whether their agreement should be revised. The deputy head of the Justice Department's Office of Legal Counsel testified to the Intelligence Committee that she would not rely on this opinion today, but I remain concerned that other government officials may be tempted to rely on it in the future. I will continue to press the Justice Department to release this opinion, so that Congress and the public can debate this bill with a full understanding of the facts. And I look forward to working with my colleagues to revise this legislation to ensure that Americans' privacy rights and American cybersecurity are both adequately protected.