WIRED

Cisa Security Bill: An F For Security But An A+ For Spying

Andy Greenberg

March 20, 2015

When the Senate Intelligence Committee passed the Cybersecurity Information Sharing Act by a vote of 14 to 1, committee chairman Senator Richard Burr argued that it successfully balanced security and privacy. Fifteen new amendments to the bill, he said, were designed to protect internet users' personal information while enabling new ways for companies and federal agencies to coordinate responses to cyberattacks. But critics within the security and privacy communities still have two fundamental problems with the legislation: First, they say, the proposed cybersecurity act won't actually boost security. And second, the "information sharing" it describes sounds more than ever like a backchannel for surveillance. On Tuesday the bill's authors released the full, updated text of the CISA legislation passed last week, and critics say the changes have done little to assuage their fears about wanton sharing of Americans' private data. In fact, legal analysts say the changes actually widen the backdoor leading from private firms to intelligence agencies. "It's a complete failure to strengthen the privacy protections of the bill," says Robyn Greene, a policy lawyer for the Open Technology Institute, which joined a coalition of dozens of non-profits and cybersecurity experts criticizing the bill in an open letter earlier this month. "None of the [privacy-related] points we raised in our coalition letter to the committee was effectively addressed." The central concern of that letter was how the same data sharing meant to bolster cybersecurity for companies and the government opens massive surveillance loopholes. The bill, as worded, lets a private company share with the Department of Homeland Security any information construed as a cybersecurity threat "notwithstanding any other provision of law." That means CISA trumps privacy laws like the Electronic Communication Privacy Act of 1986 and the Privacy Act of 1974, which restrict eavesdropping and sharing of users' communications. And once the DHS obtains the information, it would automatically be shared with the NSA, the Department of Defense (including Cyber Command), and the Office of the Director of National Intelligence.

Unfiltered Oversharing

In a statement posted to his website yesterday, Senator Burr wrote that "Information sharing is purely voluntary and companies can only share cyber-threat information and the government may only use shared data for cybersecurity purposes." But in fact, the bill's data sharing isn't limited to cybersecurity "threat indicators"—warnings of incoming hacker attacks, which is the

central data CISA is meant to disseminate among companies and three-letter agencies. OTI's Greene says it also gives companies a mandate to share with the government any data related to imminent terrorist attacks, weapons of mass destruction, or even other information related to violent crimes like robbery and carjacking. The latest update to the bill tacks on yet another kind of information, anything related to impending "serious economic harm." All of those vague terms, Greene argues, widen the pipe of data that companies can send the government, expanding CISA into a surveillance system for the intelligence community and domestic law enforcement.

"CISA goes far beyond [cybersecurity], and permits law enforcement to use information it receives for investigations and prosecutions of a wide range of crimes involving any level of physical force," reads the letter from the coalition opposing CISA. "The lack of use limitations creates yet another loophole for law enforcement to conduct backdoor searches on Americans—including searches of digital communications that would otherwise require law enforcement to obtain a warrant based on probable cause. This undermines Fourth Amendment protections and constitutional principles." Even when it comes to cybersecurity data-sharing, privacy advocates say CISA would give companies a legal loophole to mix users' personal information into the "cyber threat indicators" they pass on to federal agencies. The bill does have a provision designed to filter "personally identifiable information" out of that data. But it's far too weak as written, says Julian Sanchez, a research fellow at the CATO institute. He points to the language in the bill that calls on companies to "to assess whether [a] cyber threat indicator contains any information that the entity knows at the time of sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat and remove such information." That "knows at the time of sharing" phrase, Sanchez argues, means that companies can share personal information they haven't yet proven to be unrelated to a cyber threat. And that's especially impractical given CISA's purpose of spreading initial warnings of a possible threat quickly enough to prevent it, often before it's been fully analyzed. Take the example of a distributed denial of service attack designed to knock a target website offline with a stream of junk data. Sophisticated DDOS attacks often impersonate legitimate traffic, raising the risk that innocent traffic—and identifying IP addresses—would be included in data shared with the government. "At the time of sharing it will be very unclear if it's innocent activity," says Sanchez. "And there's no obligation to do due diligence to figure out if it's innocent or isn't."

The bill's authors have been careful to note that it doesn't compel companies to give any data to the government. A member of Senator Burr's legislative staff repeated in an email to WIRED that it merely provides a "framework" for voluntary data sharing, and added that business groups like the Financial Services Roundtable and the National Cable & Telecommunications Association have already expressed their support for the bill. "Bottom line — the bill doesn't give any government agency additional authority to collect information," wrote the spokesperson. Careful companies, of course, could in fact choose to safeguard their users' privacy beyond the requirements of CISA. But Cato's Sanchez argues that many companies seeking CISA's security benefits will take the path of least resistance and share more data rather than less, without comprehensively filtering it of all personal information. "The easiest, fastest way to share information is to select all and copy-paste. Every additional filter is an extra effort," he says. "There's no incentive to combat the tendency to err on the side of oversharing."

More False Warnings Than Real Threats

For those who value security over privacy, CISA's surveillance compromises might seem acceptable. But questions persist about whether CISA would even do much to improve security. Robert Graham, a security researcher and an early inventor of intrusion prevention systems, says CISA will lead to sharing of more false positives than real threat information. Skilled hackers, he says, know how to evade intrusion prevention systems, intrusion detection systems, firewalls, and antivirus software. Meanwhile, most data alerts from systems shared under CISA will be false alarms. "If we had seen the information from the Sony hackers ahead of time, we still wouldn't have been able to pick it out from the other information we were getting," Graham says, in reference to the epic hack of Sony Pictures Entertainment late last year. "The reality is that even if you have the information ahead of time, you really can't pick the needle from the haystack." Graham points to the more informal information sharing that already occurs in the private sector thanks to companies that manage the security large client bases. "Companies like IBM and Dell SecureWorks already have massive 'cybersecurity information sharing' systems where they hoover up large quantities of threat information from their customers," Graham wrote in a blog post Wednesday. "This rarely allows them to prevent attacks as the CISA bill promises. In other words, we've tried the CISA experiment, and we know it doesn't really work." In his statement excoriating CISA last week, Senator Ron Wyden—the only member of the intelligence committee to vote against the bill—agreed. He wrote that CISA not only lacks privacy protections, but that "it will have a limited impact on US cybersecurity." But Wyden went further than calling CISA ineffective. Citing its privacy loopholes, he questioned the fundamental intention of the legislation as it's currently written. "If information-sharing legislation does not include adequate privacy protections then that's not a cybersecurity bill," he wrote. "It's a surveillance bill by another name." Read the full bill's text, with changes from last week's amendments highlighted by the Open Technology Institute, below.

CISA bill text with OTI redlines