the Atlantic

Paranoia About CISPA Is Justified

APR 27 2012, 10:42 AM ET
CONOR FRIEDERSDORF

Recent precedent shows that even when the privacy of Americans is unlawfully violated, the interlopers never pay a price.

Reuters

On Thursday evening, the House of Representatives passed legislation called the Cyber Intelligence Information Sharing Protection Act, or CISPA. Sponsors of the bill say its purpose is to permit the government and private companies to share information with one another in order to thwart cyberthreats that could imperil national security. For example, say that spies in China were trying to hack into the personal email accounts of various government officials, the server of a hospital, or the database of a "too big to fail" bank. If CISPA is signed into law, these entities and the federal government would be able to share customer data "to identify and obtain cyber threat information," even if that data is currently unlawful to reveal (thanks to laws passed to ensure that companies don't share sensitive consumer information with the government).

Civil-liberties groups have various objections to the bill.

The ACLU conjures up a problematic scenario that could happen if it passes. "Imagine you are emailing your doctor from your Gmail account about a medical condition. Your doctor pulls up your medical records from his cloud storage server and sends them your way. Somewhere in that communication, a virus crops up," staffer Zachary Katznelson writes. "Under CISPA, Google could

send your emails, including the electronic copy of your medical records, to the NSA, so they can gather information on the virus. But, Google would be under no obligation whatsoever to scrub out your private details -- which have nothing to do with the virus. And now your medical records are in government hands indefinitely -- and the government can use them."

Before the House vote, backers of the bill were considering various amendments to address the concerns of privacy advocates and civil libertarians. The Cato Institute's Julian Sanchez articulatestheir mistake. "Instead of indiscriminately adding a cyber-security loophole to every statute on the books, why not figure out which specific kinds of information are useful to security professionals without compromising privacy, figure out which laws raise obstacles to that sharing, and then craft appropriately narrow exemptions?" he writes. "The exceptions could be appropriately narrowly tailored depending on the sensitivity of the information involved."

In other words, rather than establish the general standard that invoking national security justifies ignoring privacy laws, why not say that everyone enjoys existing privacy protections, except in a very few specific circumstances when very specific types of customer information can be shared? As Scott M. Fulton puts it at *Read Write Web*, "The privacy of American citizens and the national security of the United States are too important to be left to intentionally vague regulations and legislation." He goes on to suggest that lawmakers should "stipulate that these are the circumstances in which exceptions must be made to protect vital national security interests. Then, establish an audit trail. State that all transactions must be registered, and the log of those registries may be obtained by public request, pending the approval of a judge."

Which is to say, if we're going to allow private companies and government to snoop into our private information for the narrow purpose of protecting national security, there needs to be a way to monitor what goes on so that there's at least the possibility that abuses could be caught.

WHY NEITHER INDUSTRY NOR GOVERNMENT CAN BE TRUSTED

Critics of CISPA are right to be wary, for all of the aforementioned reasons specific to the legislation -- but also because of the abysmal record that government and industry have amassed lately. The Bush Administration engaged in illegal warrantless wiretapping for years. All the while, the National Security Agency collaborated with America's major telecommunications companies. AT&T gave government officials unsupervised access to all data flowing through major hubs, including email messages, phone calls, web-browsing data, and private network traffic.

When the NSA program was finally revealed, Bush Administration officials weren't prosecuted and jailed. In fact, Thomas Drake, an NSA whistleblower who complained about a separate warrantless surveillance project, was prosecuted by both the Bush and the Obama Administrations.

This helps explain why civil libertarians are perturbed. Take Sanchez. Explaining why he wasn't satisfied by some of the last minute safeguards added onto CISPA, he cited recent history:

When civil liberties advocates cried foul at the prospect of such vast quantities of private data being handed over to government on a silver platter, the bill's supporters tried to placate them by tacking on an array of after-the-fact anonymization requirements and use restrictions -- forbidding the use of the data except for a "cybersecurity purpose" or for "the protection of the national security of the United States."

That wasn't much consolation to anyone who's watched how the government has tried to interpret similar "purpose" restrictions in the past. In 2002, for example, then-Solicitor General Ted Olson argued for a highly expansive view of the "foreign intelligence purposes" for which information obtained through national security wiretaps could be used, including using evidence of misconduct unrelated to terrorism or espionage to force people to become informants. If a wiretap turned up evidence of tax evasion or rape, for instance, Olson suggested the government "could go to that individual and say we've got this information and we're prosecuting and you might be able to help us. I don't want to foreclose that." It's no great leap to imagine a future solicitor general arguing that extorting the cooperation of hackers, penetration testers, or other tech professionals would similarly serve a "cybersecurity purpose."

In a statement objecting to CISPA as currently written, the Obama Administration stated that "citizens have a right to know that corporations will be held legally accountable for failing to safeguard personal information adequately." Damn right they do! But Obama has done nothing to hold anyone accountable for spying on Americans during the Bush years. And Bush-era abuses -- coupled with the failure to hold anyone accountable for them, the prosecution of whistleblowers, and ongoing warrantless surveillance -- are indirectly but powerfully relevant to CISPA.

The legislation is trying to strike a balance: to permit government access to potentially sensitive information without making citizens vulnerable to dangerous abuses. Before the Bush Administration's illegal spying, it was easy to imagine that the legal penalties for exceeding the bounds of the law would be one check on government officials and corporate leaders tempted to abuse their access to data. We now know that when national security is invoked, these people are treated as if they're above the law. If legal violations aren't going to be punished after the fact, it's prudent for concerned citizens to push for even more elaborate preemptive safeguards.