techdirt

There Is A 'Right Way' To Do Cybersecurity Information Sharing, But CISPA Is Not It

from the *sharing-is-caring* dept

We've argued, repeatedly, that the backers of various cybersecurity bills have failed to give a real reason for *why* such bills are needed. What is the imminent threat and why does it need legislation? The only point of issue that has made some sense is that you *can* envision areas where it would be quite useful for companies and governments to share *specific* threat- or attack-related information, for the purpose of stopping that (or related) threats and attacks. But that's a very limited scenario. The entire framework of CISPA ignores that, which is why it's unclear if the bill even **could** be fixed. That said, Julian Sanchez, over at the Cato Institute, has posted an interesting analysis of **what information sharing regulation should look like**. First, he discusses the problem with the CISPA setup:

CISPA worked by creating a sweeping exception to all other privacy and surveillance laws, granting blanket immunity to any "entity" that chose to share vaguely defined "cyber threat information"—potentially including the contents of e-mails or other online communications—with both private actors and the government. 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."

Basically, take a broad, vaguely defined law for a specific purpose... but leave it open to allowing the government to stretch that definition, and the government will almost always do so.

But, again, you can see cases where information sharing could be useful, so Sanchez suggests what might make sense there:

*Instead of indiscriminately adding a cybersecurity 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? (One assumes the intelligence agencies can be afforded more discretion about when to share the information already in their own possession—whatever else one might say about it, "oversharing" is not among the NSA's problems.)*

The exceptions could be appropriately narrowly tailored depending on the sensitivity of the information involved. For instance, different sections of the Electronic Communications Privacy Act deal with different kinds of data. Subsections (1) and (2) of 18 USC §2702 deal with the contents of communications in transit through or stored by a communications provider, generally prohibiting use or disclosure of that information without specific consent. Subsection (3) covers subscriber information and transactional data about those communications, and generally permits voluntary sharing, but specifically prohibits sharing with governmental entities. Since that transactional information is typically less sensitive than communications themselves, an exemption there might allow providers a fair amount of discretion to determine what constitutes "cyber threat information" and permit sharing with government also, subject to the appropriate anonymization and use requirements. For the more sensitive contents, the exception might be limited to a relatively specific laundry list of kinds of data that are both unquestionably security-related and limited in their implications for privacy, such as malware signatures and attack payloads.

In other words, let's more carefully define the real problem here. The government is insisting that information needs to be shared, but that's not "the problem." Information can be shared already. The reason that CISPA works by creating a huge immunity umbrella is that the "problem" with sharing isn't that information can't be shared, but that certain already overburdensome regulations block certain kinds of sharing in situations where it makes sense. The answer isn't to remove all liability for the oversharing of info, but to narrowly create exceptions to where key information that actually is necessary to be shared can have that done without violating the law. In other words, as you dig deeper, it appears that the problem isn't about sharing information -- it's about a series of existing laws that failed to take into account future realities. So, a much more targeted and reasonable solution is to figure out *exactly* where that friction is, and to clear out those blockages. But, that's not what CISPA does.