WIRED

CISPA Is Dead. Now Let's Do a Cybersecurity Bill Right

By: Julian Sanchez – April 26, 2013

The controversial Cyber Intelligence Sharing and Protection Act (CISPA) now appears to be dead in the Senate, despite having passed the House by a wide margin earlier this month. Though tech, finance, and telecom firms with a combined $650 million in lobbying muscle supported the bill, opposition from privacy groups, internet activists, and ultimately the White House (which threatened to veto the law) seem to have proven fatal for now.

For all the heated rhetoric surrounding the CISPA legislation — predictions of an impending Digital Pearl Harbor matched by dire warnings of Big Brother surveillance — the controversy was almost entirely unnecessary.

Americans have grown so accustomed to hearing about the problem of "balancing privacy and security" that it sometimes feels as though the two are always and forever in conflict — that an initiative to improve security can't possibly be very effective unless it's invading privacy. Yet the conflict is often illusory: A cybersecurity law could easily be drafted that would accomplish all the goals of both tech companies and privacy groups *without* raising any serious civil liberties problems.

Few object to what technology companies and the government say they want to do in practice: pool data about the activity patterns of hacker-controlled "botnets," or the digital signatures of new viruses and other malware. This information poses few risks to the privacy of ordinary users. Yet CISPA didn't authorize only this kind of narrowly limited information sharing. Instead, it gave companies blanket immunity for feeding the government vaguely-defined "threat indicators" — anything from users' online habits to the contents of private e-mails — creating a broad loophole in all federal and state privacy laws and even in private contracts and user agreements.

Given that recent experience has shown companies shielded by secrecy often err on the side ofoversharing with the government, that loophole was a key concern. So why the gap between what the law permits and its supporters' aims?

It's a principle wonks call tech neutrality. Nobody wants to write a bill that refers too specifically to the information needed to protect *current* networks (like "Internet Protocol addresses" or "Netflow logs") since technological evolution would render such language obsolete over time.

Unfortunately, the alternative has been to extend a broad, vague immunity for sharing and attach a series of back-end restrictions designed to prevent misuse.

Fortunately, there's a better way: A law embodying three simple principles could permit all the sharing that's actually useful for security purposes … *without* compromising privacy.

Respect Contractual Agreements With Users

CISPA's broad immunity effectively overrode contractual promises*not* to share particular types of data. A more limited immunity would not only create space for diverse users and companies to determine what degree of information sharing they find acceptable, it would also compensate for the vagueness inherent in CISPA's broad tech neutral definitions.

Instead of creating an indiscriminate loophole, a new and improved CISPA should establish immunity from state and federal criminal statutes that limit information sharing by communications service providers — but require the companies to "opt in" to the protection by giving users more specific details about the categories of information they intend to share.

This approach leaves the *statutory* definitions flexible enough to deal with evolving technology, but guarantees users will have clear notice of what companies plan to share and advance warning if some seem disposed to overshare. Companies would then have some market incentive not to disclose more than is really necessary for security purposes, and users would retain a legal mechanism to punish companies that break their own privacy promises.

Strip Out Personal Information From Shared Data

Companies — not the government — should be responsible for stripping out personal information from their data *before* it's shared, as they've already said they're perfectly capable of doing. There's no need to share such data for security purposes anyway: Kevin Mandia, head of the cybersecurity firm Mandiant, insisted at a February hearing on CISPA that in 20 years in the industry, he had "never seen a package of threat intelligence that's actionable" that included personally identifiable information.

Of course, some kinds of theoretically anonymous information — such as IP addresses — are useful for security but also capable of being tied back to individual users if linked with other databases.

To ensure that anonymous data stays anonymous, the law should limit the sharing of raw data to a designated civilian agency, like the Department of Homeland Security, and ensure that only *aggregate information or derivative analyses* are subsequently shared with entities like the National Security Agency, whose vast trove of data might allow them to tie numbers to names.

Erase the Data

Information shared with the government should come stamped with what geeks call time-to-live (TTL), a marker that tells a computer system when a particular packet of data should be automatically erased.

The primary purpose of information sharing is to provide a real-time early warning system that could detect patterns suggesting an impending attack before it happens. But

that data has little practical use a week or two after the fact — which means there's no legitimate cybersecurity purpose served by retaining it longer than that.

When particular types of data are needed for longer — the government begins a criminal investigation into an attack, for instance — current law gives law enforcement ample recourse. They already have the power to issue "preservation orders" requiring private companies to hang on to data that may be useful in an investigation, data which can then be obtained using traditional tools like subpoenas and court orders. And victims of an attack (as opposed to their internet provider) can already share data without such restrictions.

Mandating a TTL for CISPA-shared information avoids what is probably the central civil concern about the law: that it would lead to the creation of a vast database of detailed information about internet activity — one that would eventually tempt the government to use it for other purposes.

***

With these features, new legislation would achieve all the essential aims of CISPA's sponsors — while leaving civil libertarians with little to object to.

That lawmakers haven't already simply incorporated such safeguards suggests that perhaps they, too, have fallen victim to zero-sum thinking about privacy and security, wrongly assuming that less of the former automatically yields more of the latter.

The sooner they — and we — recognize that fallacy, the sooner Americans can get legislation that protects both.