ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

April 25, 2012 | By Trevor Timm

CISPA, "National Security," and the NSA's Ability to Read Your Emails

This week the House of Representatives is debating CISPA, the dangerous 'cybersecurity' bill that threatens to decimate Internet users' privacy in the name of security. EFF and a wide variety of other groups have been protesting the law's provisions giving companies the power to read users' emails and other communications and hand them to the government without any judicial oversight whatsoever—essentially a giant 'cybersecurity' exception to all existing privacy laws.

We've already shown how the bill's definition of 'cyber threat information' can lead the companies and government to surveil citizens for a host of reasons beyond critical cybersecurity threats. But we want to focus on one vital portion of the bill that is not getting enough attention: what the government can do with your private information once companies hand it over.

Even though CISPA is styled as a 'cybersecurity' bill, it explicitly allows the Department of Homeland Security and other government agencies like the National Security Agency (NSA) to use your information for 'national security' purposes—expanding the bill far beyond its purported goal. Bill sponser Mike Rogers introduced a package of amendments yesterday, but did not remove "national security" as one of the purposes for which information can be used.

The Erosion of Civil Liberties

In the past decade, the amorphous phrase "national security" has invaded many arenas of government action, and has been used to justify much activity that did not involve legitimate terrorist threats. The most obvious (and odious) example is the unfortunately named USA-PATRIOT Act, a law that was sold to the American public as essential to combating terrorism, but which has overwhelmingly been applied to ordinary American citizens never even suspected of terrorism.

In just one of many examples, from 2003-2006, the FBI issued more than 192,000 National Security Letters to get Americans' business, phone or Internet records without a warrant. These invasive letters—which come with a gag order on the recipient so they can't even admit they received one—have been used to gather information about untold number of ordinary citizens, including journalists. Exactly one of those cases ended in a terrorism conviction—and he would have been convicted without the NSL evidence. The ACLU has catalogued how many other PATRIOT Act provisions have been similarly abused. EFF is suing for information about one provision, known as Section 215, which Senators have warned is being secretly interpreted to invade privacy in a way that "most Americans would be stunned" to learn about.

"Information sharing"— CISPA's mantra—has also created privacy nightmares for everyday Americans in the name of national security. The federal government routinely shares its massive national security databases with local law enforcement agencies with predictable results. An investigation by PBS Frontline and the Washington Post's Dana Priest showed that "many states have yet to use their vast and growing anti-terror apparatus to capture any terrorists; instead the government has built a massive database that collects, stores and analyzes information on thousands of U.S. citizens and residents, many of whom have not been accused of any wrongdoing."

Despite the ample evidence of these expansive "national security" powers being used on ordinary citizens, the government has only continued down the same path. Just last month, the National Counterterrorism Center drastically changed its rules so it can now copy entire data bases from other federal government agencies and keep information on citizens for up to five years—even if they're completely innocent.

Wrongdoing and Abuse Go Unchecked

Of course, with such unchecked power, abuse is inevitable. In 2010, EFF learned through Freedom of Information Act requests indications that the FBI—one of the many agencies that might receive private communications via CISPA—may have committed upwards of 40,000 possible intelligence violations in the nine years since 9/11—many of which were done under the PATRIOT Act. In addition, we've found evidence of the FBI "lying in declarations to courts, using improper evidence to obtain grand jury subpoenas, and accessing password-protected files without a warrant."

Incredibly, it recently emerged the FBI may have not only condoned this type of behavior, but *encouraged* it. Wired recently published an FBI memo on agent training that said, "Under certain circumstances, the FBI has the ability to **bend or suspend the law** and impinge on freedoms of others" and cited various wiretapping laws in national security investigations. (emphasis ours)

Increased powers of the National Security Agency

CISPA's author Rep. Mike Rogers has tried to stave off criticism of that CISPA would lead to government abuse by insisting that the bill allows citizens to sue the government if they misuse their information. But this provides very little comfort. Any such lawsuit will be difficult, if not impossible, to bring. The government can attempt to use the same "national security" exception in CISPA that allows them to use the information for other purposes to escape liability.

First, the statute of limitations for such a lawsuit is two years from the date of the actual violation. It's not at all clear how an individual would know of such misuse if it were kept inside the government. Given that the National Security Agency is notoriously secretive—its employees even used to refer to it as "No Such Agency"—they may attempt to prevent users from finding out exactly how this information was ever used. And a provision in CISPA that provides an exemption to the Freedom of Information Act for all private information handed over by companies for anything cybersecurity related will just make it harder.

But even if a user knew the government was misusing his or her information, litigation would be difficult, expensive, and time consuming given if classified information or national security is involved, the government may invoke the "state secrets privilege."

EFF has been involved for years in a lawsuit over Fourth Amendment and statutory violations stemming from *another* abuse of the government's claimed 'national security' powers—the NSA's warrantless wiretapping program. Given the NSA may be a recipient of "cyber threat information" in CISPA, they stand to gain more power to spy on Americans despite laws that would otherwise prevent them from doing so.

Despite six years of litigation, the government continues to maintain that the "state secrets" privilege prevents lawsuits over the warrantless wiretapping program from being heard, arguing that *even if the allegations are true*, the suit should be dismissed because of—you guessed it—national security concerns. The same state secrets privilege has been invoked in other cases involving the CIA's extraordinary rendition program and their authority to target Americans in drone strikes overseas with no judicial safeguards.

CISPA will create yet another tool for the government to expand its already massive national security apparatus, and in turn, erode ordinary citizens' rights, while giving them virtually no recourse if their civil liberties are violated. The House of Representatives is beginning debates on CISPSA tomorrow, with a vote coming no later than Friday. Join EFF in opposing CISPA by calling, emailing, and tweeting at your Representatives.

https://www.eff.org/deeplinks/2012/04/cispa-national-security-and-nsa-ability-read-your-emails