Cybersecurity Information-Sharing Legislation:
Sharing Cyber Threat Indicators (CTIs)—Separating Fact From Fiction

August 19, 2015

Some privacy and civil liberties groups perpetuate the falsehood that personal information is typically necessary to identify cyber threats. This position is inaccurate and being used to oppose needed cybersecurity information-sharing legislation, particularly S. 754, the Cybersecurity Information Sharing Act (CISA) of 2015, which the Protecting America's Cyber Networks Coalition is pressing the Senate to vote on in the fall.

CISA's definition of cyber threat indicators (CTIs) limits the information that can be shared by businesses and government entities to essentially identify and help defend against the tactics, techniques, and procedures used by malicious actors to compromise the computer networks of their victims—not sensitive personal information contained in such networks.

CTIs, according to the bill, describe or identify malicious reconnaissance, a method of defeating a security control or exploitation of a security vulnerability, malicious cyber command and control, the actual or potential harm caused by an incident, among other types of cyber threat data. Listed below are some common examples of clinical information that comprise CTIs, which in the vast majority of cyber incidents do not implicate a person's behavioral, financial, or social information.

Select Examples of CTIs

- **Domain names** refer to the location of an organization on the Internet.
- **Internet protocol (IP) addresses** are unique numerical identifiers assigned to every computing device connected to the Internet.
- **Log data** can be thought of as the exhaust gas of an information system and often reveals clues associated with a cyberattack.
- **Malware** includes viruses, worms, and Trojan horses. Methods of delivering malware include **botnets,** a type of malware that allows an attacker to take control of an infected computer and launch **phishing attacks.** Cybercriminals send out waves of spam email in hopes of "hooking" an unsuspecting individual into clicking on an infected attachment or Web link in an email.
- All communications on the Internet are broken up into **packets** when they are transmitted from, for example, a smartphone to a laptop computer; the packets are reassembled when they reach the destination computer. Each packet contains "header" information, comparable to the outside of a mailing envelope, which includes IP addresses.
- Computers use different **ports** to handle various types of Internet traffic (e.g., email traffic is handled on certain ports, while website traffic is handled on others). Port information does not reveal traffic contents.
- **Signatures** refer to recognizable, distinguishing patterns associated with a cyberattack (e.g., a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a network).
- **Time/date stamps** are used to identify the timing of a cyberattack.
- **Uniform Resource Locator (URL)** is a Web (www) address.

In those rare instances where an individual's personal information might happen to be embedded within CTIs or defensive measures, CISA mandates that public and private entities remove such personal information unrelated to a cyber threat when sharing CTIs and defensive measures.

The bottom line is that CISA is about protecting America's cyber systems. It is not a surveillance bill, which some privacy advocates wrongly argue by stretching the intent of CISA to unrecognizable lengths. The fact is that CISA does not authorize the government to surveil individuals or target crimes unrelated to cybersecurity.

First, a revised version of CISA eliminates the government's ability to use CTIs to investigate and prosecute "serious violent felonies"—which is a significant privacy-enhancing change to the bill.

Second, CISA provides authorization for a company to monitor its own network, including the information stored on, processed by, or transiting its own network, as well as the information on the network of another entity with which it has a written contractual agreement—but only for "cybersecurity purposes." Further, monitoring under CISA is not intended to equate the meaning of "monitoring" as used in the context of federal criminal wiretap law or electronic surveillance under the Foreign Intelligence Surveillance Act (FISA). Any other monitoring by companies would require authorization beyond what CISA grants.

Third, Senator Dianne Feinstein (D-CA), the bill's co-author, said on the Senate floor on August 5 that CISA is not a surveillance bill, and that the bill was amended several times to address critics' concerns:

> [CISA] is not a surveillance bill. . . . It gives the Attorney General [and the Secretary of Homeland Security] the obligation to come up with secure guidelines to protect private information. . . . We have taken every step to prevent privacy violations from happening under this bill. Yet there are individuals who still raise that as a major concern. *I believe it is bogus.* I believe it is a detriment to us in taking this first step to protect our American industries. If we don't pass it, the thefts are going to go on and on and on [italics added].

Senator Feinstein is not alone among lawmakers in making sharp distinctions between surveillance programs and CISA. In March, the House Intelligence Committee passed H.R. 1560, which is similar to CISA. Ranking Member Adam Schiff (D-CA) stressed, "No one is a bigger advocate for NSA [National Security Agency] reform than I've been." He said that he sees the NSA issues as separate from cyber information-sharing legislation, where "we've done everything we can to meet the demands of the privacy community."[*]

Businesses and Privacy Advocates Share a Common Adversary

The real assault against individuals' privacy is coming from a mutual foe—foreign powers or their proxies and cybercriminals that steal daily our login credentials, payment card data, trade secrets, and much more to cause tangible and costly harm to citizens, consumers, and businesses. To this extent, industry believes that privacy advocates should join businesses in pushing for CISA's passage.

The bipartisan CISA bill has been carefully written to guard privacy, preserve the role of civilian and intelligence agencies, and spur public-private sharing of cyber threat data with appropriate liability protections for companies. The business community urges the Senate to bring up CISA and pass it after it returns from the August recess.

[*] See "House Intelligence leaders seek to defuse privacy concerns around cyber info-sharing," *Inside Cybersecurity*, March 27, 2015. http://insidecybersecurity.com/daily-news/house-intelligence-leaders-seek-defuse-privacy-concerns-around-cyber-info-sharing.

Agricultural Retailers Association (ARA)
Airlines for America (A4A)
Alliance of Automobile Manufacturers
American Bankers Association (ABA)
American Cable Association (ACA)
American Chemistry Council (ACC)
American Fuel & Petrochemical Manufacturers (AFPM)
American Gaming Association
American Gas Association (AGA)
American Insurance Association (AIA)
American Petroleum Institute (API)
American Public Power Association (APPA)
American Water Works Association (AWWA)
ASIS International
Association of American Railroads (AAR)
Association of Metropolitan Water Agencies (AMWA)
BITS–Financial Services Roundtable
College of Healthcare Information Management Executives (CHIME)
CompTIA–The Computing Technology Industry Association
CTIA–The Wireless Association
Edison Electric Institute (EEI)
Electronic Payments Coalition (EPC)
Electronic Transactions Association (ETA)
Federation of American Hospitals (FAH)
Food Marketing Institute (FMI)
Global Automakers
GridWise Alliance
HIMSS–Healthcare Information and Management Systems Society
HITRUST–Health Information Trust Alliance
Large Public Power Council (LPPC)
National Association of Chemical Distributors (NACD)
National Association of Manufacturers (NAM)
National Association of Mutual Insurance Companies (NAMIC)
National Association of Water Companies (NAWC)
National Business Coalition on e-Commerce & Privacy
National Cable & Telecommunications Association (NCTA)
National Rural Electric Cooperative Association (NRECA)
NTCA–The Rural Broadband Association
Property Casualty Insurers Association of America (PCI)
The Real Estate Roundtable
Software & Information Industry Association (SIIA)
Securities Industry and Financial Markets Association (SIFMA)
Society of Chemical Manufacturers & Affiliates (SOCMA)
Telecommunications Industry Association (TIA)
Transmission Access Policy Study Group (TAPS)
United States Telecom Association (USTelecom)
U.S. Chamber of Commerce
Utilities Telecom Council (UTC)