Cybersecurity Information-Sharing Legislation: It's About Protecting America's Cyber Networks, *Not* Surveilling You

August 10, 2015

Some privacy groups perpetuate the myth that personal information is typically necessary to identify cyber threats, and that cybersecurity information-sharing legislation is equal to surveillance. The caption below isn't a series of typos. It shows a typical example of cyber threat information—technical and sterile data—that businesses share and receive from industry and government partners to counter cyberattacks. It contains no personal information—and that's the point.

```
#NCF Dec 27 2012—DDoS Rules

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ZBC DDoS - HTTP Header Structure with
Hex Byte URI seen"; flow:established,to_server; content:"Keep-Alive|3a 20|"; http_header; fast_pattern; content:!"gzip";
http_header; content:"Connection|3a 20|Keep-Alive"; http_header; nocase; pcre:"/[\?&][a-f0-9]{5,6}$/U"; classtype:web-
application-attack; sid:40000006; rev:4;)
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ZBC DDoS - KamiKaze";
flow:established,to_server; content:"CLIENT-IP|3a 20|"; http_header; fast_pattern; content:"Via|3a 20|"; http_header;
content:"X-FORWARDED-FOR|3a 20|"; http_header; classtype:web-application-attack; sid:40000007; rev:1;)
```

The surveillance myth and other falsehoods are used to oppose positive information-sharing legislation, particularly S. 754, the Cybersecurity Information Sharing Act (CISA) of 2015, which the Senate is expected to vote on in the fall. To set the record straight, it is important to debunk five myths held by a small, but vocal, group of lawmakers and privacy interests.

Myth: Shared cyber threat information is broad in scope.

Fact: CISA's definition of cyber threat indicators (CTIs) is very limited. Businesses and government entities may only share the tactics, techniques, and procedures used by malicious actors to compromise the computer networks of their victims. In the vast majority of cyber incidents, CTIs do not implicate a person's behavioral, financial, or social information.

Myth: CISA is a surveillance bill.

Fact: CISA does not authorize the government to surveil individuals, such as targeting 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 pro-privacy change to the bill.

Second, network "monitoring" conducted by businesses under CISA is limited to cybersecurity purposes, similar to CTIs. Monitoring can only be conducted on a company's *own* information systems. 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, a California Democrat, 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].

Myth: The bill allows companies to use offensive measures or "hack back."

Fact: CISA does not permit so-called hacking back—companies are not authorized to destroy or render computer systems unusable. The bill ensures that "defensive measures" (DMs) are properly bounded. The managers' amendment clarifies that companies are not allowed to gain unauthorized access to a computer network.

Myth: CISA does not require businesses to remove personal data from threat indicators.

Fact: CISA contains multiple, overlapping provisions to guard and respect privacy. For example, in those rare instances where an individual's personal information is embedded within CTIs or defensive measures, CISA calls for public and private entities to *remove such personal information* unrelated to a cyber threat when sharing CTIs and DMs—and the federal government must do the same.

Myth: Businesses are encouraged to share information with the Department of Defense (DoD) and the National Security Agency (NSA).

Fact: Businesses are not granted liability protection when sharing CTIs with the DoD and the NSA—which preserves the status quo. CTIs that businesses pass on to the federal government must go through the Department of Homeland Security (DHS), which is a civilian entity.

***

CISA's authors, Senators Richard Burr, a Republican from North Carolina, and Feinstein, have recently revised their bill to increase its privacy protections. Among other things, the managers' amendment further limits the sharing of cyber threat data to "cybersecurity purposes." Closely related, the revised measure eliminates the government's use of cyber threat indicators to investigate and prosecute "serious violent felonies," thus putting to rest false claims that CISA is a surveillance bill. The managers' amendment also ensures that the use of DMs does not allow an entity to gain unauthorized access to a computer network. The bill writers have worked diligently to address the concerns of privacy and civil liberties organizations.

CISA passed the Senate Select Committee on Intelligence in March with broad support from both political parties and industry. The bipartisan bill would help businesses achieve timely and actionable situational awareness to improve theirs and the nation's detection, mitigation, and response capabilities against cyber threats. CISA represents a workable compromise among many stakeholders. CISA safeguards privacy and civil liberties; it is not a surveillance bill.

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)