Cybersecurity Information-Sharing Legislation: 'Voluntary' Means Voluntary—Separating Fact From Fiction

August 26, 2015

Some privacy and civil liberties advocates say that the biggest myth surrounding the Cybersecurity Information Sharing Act (CISA) of 2015 (S. 754) is it would be voluntary. According to one writer:

> Nothing in the *letter or spirit* of CISA . . . would prevent DHS [Department of Homeland Security] from establishing a similar compulsory process, all while trumpeting the 'voluntary' nature of the program. In fact, the 'cyber threat information' that the government would be allowed to share with participating companies under the bill may, and foreseeably will, provide so much of a competitive advantage—the advantage of being 'in the know'—that companies will be *forced* to participate simply to keep up with their participating competitors. Not to comply might actually harm their corporate interests and put their customers at risk. A world where a company is *forced* to betray its users in order to protect them is backward indeed [italics added].

This line of thinking seriously misses the voluntary nature of CISA and is worth critiquing on three fronts. First, members of the Protecting America's Cyber Networks Coalition (the coalition) and many other cybersecurity stakeholders have successfully pressed Congress from the outset to write legislation in a way that would restrict the government from compelling companies to turn over data of any kind. To this extent, industry and privacy groups agree on the critical point that companies must not be forced to report to the government. We also believe, as privacy advocates surely do, that foreign governments must not enact cyber threat-sharing laws obliging companies to turn over information.

The coalition contends that mandating the disclosure of cyber threat data and defensive measures would damage trusted relationships among businesses, consumers, and government entities that are needed to guard sensitive commercial and customer information from cyberattacks. Coalition members have productive partnerships with federal agencies and departments to help companies manage cybersecurity incidents. Reporting mandates would severely damage these relationships.

Second, CISA clearly contains language prohibiting a "new information sharing relationship" between a business and a government agency or department. The bill prevents the government from making a private entity amend or break a contract that it has with a business or government partner. CISA also contains an "anti-tasking" provision, which ensures that a business is not obliged to provide information to the federal government. Indeed, the committee report that accompanies the legislation provides another backstop, saying that CISA "creates a completely voluntary information-sharing framework." Both the letter and spirit of CISA show that "voluntary" means voluntary.

CISA is meant to be voluntary—really. (Select language from the bill.)

(f) Information sharing relationships.—Nothing in this Act shall be construed—
(1) to limit or modify an existing information sharing relationship;
(2) to prohibit a new information sharing relationship;
(3) to require a new information sharing relationship between any entity and the Federal Government; or
(4) to require the use of the capability and process within the Department of Homeland Security developed under section 5(c).
(g) Preservation of contractual obligations and rights.—Nothing in this Act shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any entities, or between any entity and a Federal entity; or
(2) to abrogate trade secret or intellectual property rights of any entity or Federal entity.
(h) Anti-Tasking restriction.—Nothing in this Act shall be construed to permit the Federal Government—
(1) to require an entity to provide information to the Federal Government;
(2) to condition the sharing of cyber threat indicators with an entity on such entity's provision of cyber threat indicators to the Federal Government; or
(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity.
(i) No liability for non-Participation.—Nothing in this Act shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this Act. (Section 8 of the bill, as reported)

Third, a proposed amendment to CISA, expected to be offered by Senator Jeff Flake (R-AZ), would apparently reinforce the voluntary essence of CISA, which is that the legislation is meant to be optional and not coercive. This amendment has a good chance of being adopted when CISA is voted on.

Text of the Senator Flake amendment

SA 2580. Mr. FLAKE submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Beginning on page 46 [of the reported bill], strike line 10 and all that follows through page 47, line 12, and insert the following:
(3) to require a new information sharing relationship between any entity and the Federal Government or another entity; or
(4) to require the use of the capability and process within the Department of Homeland Security developed under section 5(c).
(g) *Preservation of Contractual Obligations and Rights*.—Nothing in this Act shall be construed—
(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any entities, or between any entity and a Federal entity; or
(2) to abrogate trade secret or intellectual property rights of any entity or Federal entity.
(h) *Anti-Tasking Restriction*.—Nothing in this Act shall be construed to permit the Federal Government—
(1) to require an entity to provide information to the Federal Government or another entity;
(2) to condition the sharing of cyber threat indicators with an entity on such entity's provision of cyber threat indicators to the Federal Government or another entity; or
(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity or another entity.

Businesses and Privacy Advocates Agree: CISA Must be Voluntary

The coalition believes that nothing in CISA would establish a compulsory information-sharing process—which coalition members would vigorously reject. We hold that cybersecurity incident reporting is most powerful when government and industry collaborate. Public policies that attempt to compel businesses to report cybersecurity information often lead to less—not more—information sharing, compared with programs that emphasize creativity, speed, and innovation.

CISA has been thoughtfully crafted to protect individuals' privacy, while providing greater legal certainty to increase the timely exchange of actionable cyber threat information. The coalition urges the Senate to bring up CISA and pass it after it returns from the summer recess.

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 Coatings Association
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)
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)