The Intersection of Internet Freedom and Cybersecurity

David Inserra

Freedom requires that one be safe and secure in one's possessions—a world in which criminals steal or destroy one's property at will is neither free nor secure. The same is true in cyberspace, where digital criminals have a great interest in stealing sensitive data or disrupting critical services. And with everything from military systems to smartphones now linked to the Internet, the number of bad actors seeking to attack or steal from those targets has increased dramatically. Hackers compromise, steal, or destroy hundreds of billions of dollars in intellectual property and real money every year, as well as accessing critical military secrets from the United States. While different estimates exist for the cost of cybercrime, they seem to point to annual costs to the U.S. of $100 billion or more, and to global costs that could reach $600 billion.[101]

Regulatory Solution Falls Short

How can this problem be addressed? Early congressional proposals supported by the Obama Administration would have imposed mandatory cybersecurity standards on key private-sector industries.[102] Mandatory standards have certain surface appeal: After all, if security standards in the private sector are not where they should be, shouldn't the government step in and require better security? While simple in theory, this approach actually has several fatal flaws.

First, regulations will have a hard time keeping up with the rapidly changing environment. Moore's Law states that the processing power of computers will double approximately every two years—a law that has been true since the 1970s. While cyber mandates may be able to improve cybersecurity by making companies able to address threats of the last generation, they are ill prepared to address constantly changing threats that emerge from the current and future generations of technology.

Second, because of the delay inherent in government regulation, cybersecurity innovation suffers. Even if proposed regulatory proposals avoid proscribing specific solutions, they tend to focus on problems, threats, and features of cyberspace that are specific to the past. As a result, companies will seek solutions that meet the outdated regulations, at the expense of solutions for the current or foreseeable crop of problems. Thus, government regulation could actually weaken U.S. cybersecurity.[103]

Third, regulations often create a culture of compliance. Regulations ultimately require businesses to do certain things or face penalties. When faced with such prospects, many companies will seek the lowest-cost way of meeting these standards, regardless of whether such actions will be the best decision for any given company. This compliance-over-security mindset opposes innovation and real engagement with the issue at hand. As a result, regulations are a less than ideal way to encourage cost-effective investments in security.

Engaging the Private Sector

Policymakers can reduce barriers to improved cybersecurity by using private-sector incentives instead of top-down mandates. One is the sharing of cybersecurity threat and vulnerability information among both private and public-sector entities. By sharing information, different entities in the two sectors can be warned about likely attacks or other specific problems. No company or government agency knows everything about cybersecurity, which makes sharing information about threats and vulnerabilities a cost-effective way to raise cyber preparedness and awareness. Information sharing can be seen as a kind of crowdsourcing function, akin to the popular "Waze" application for traffic data, by which users voluntarily report traffic conditions they experience. Just as Waze helps large numbers of individuals on their commute, information sharing in cyberspace helps businesses and government agencies avoid cybersecurity potholes and problems, and does so at little cost.

Information sharing is a relatively inexpensive way of improving cybersecurity and it involves minimal sharing of personal information. While sensitive and personal data in e-mails and databases may be the target of cyberattacks, information sharing is not aimed at using the personal content of those e-mails and databases since that information does nothing to support security. Instead, sharing information about threats, vulnerabilities, and the source of attacks enhances and protects the privacy of Internet users.

Enabling Better Information Sharing

There are, however, a number of government-imposed obstacles that are impeding voluntary sharing of information. Policymakers should remove these obstacles by:

1. **Clarifying ambiguous laws limiting disclosures.** Currently, at least two statutes, the Wiretap Act and the Stored Communication Act arguably prohibit the sharing of cybersecurity information. Both were passed in 1986 to deal with telephone issues, prohibiting communications providers from disclosing the contents of electronic communications or information about a customer without having the appropriate authorization. This is construed by some to include the coding of viruses and malware and the IP addresses from which cyberattacks are originating. The statutes should be amended or other laws should clarify that sharing such information is not a violation.

2. **Protecting sharers from excessive liability.** In many cases under current law, a firm that shares information may find itself liable for damages if the information is relied upon by a third party, and turns out to be erroneous. Alternatively, a firm may find itself subject to a lawsuit by a party harmed by the reported cybercrime, based on alleged negligence revealed by the shared information.

   This potential liability is one of the biggest obstacles to information sharing, as firms find it less dangerous to keep information to themselves. To remove this obstacle, information sharers who act without malicious intent or gross negligence should receive protection from lawsuits that are based on the shared information. Lawsuits not using the shared information would be unaffected. This safe harbor from suit would only apply to actions based on statute or on torts. Contractual obligations, such as commitments made to consumers as part of a privacy policy, would not be affected.

3. **Protecting information from Freedom of Information Act (FOIA) requests and use by regulators.** Similar to liability protection, protection from regulatory use guarantees that a regulator will not use shared information to propose additional regulations or punish a potential failure to meet regulatory standards. Additionally, FOIA protection is also necessary because businesses do not want their competitors to get their hands on proprietary information or business dealings.

Clear and Responsible Oversight

All that said, it is important that any information-sharing proposal ensure strong oversight of the information-sharing system that is established. As with any government program, the potential for abuse is real. Personal information could be shared or used inappropriately. For this reason, the United States has placed privacy officers throughout government agencies since 9/11 to review various new security and information-sharing programs. The federal government should use this existing system of privacy officers to review sharing procedures and observe how information is being used. The Department of Homeland Security would be the most appropriate government organization to act as an information-sharing hub. Alternatively, establishing a public-private-partnership organization to act as the information-sharing hub could include privacy groups on the organization's board not only to review official sharing procedures, but also to analyze information sharing and its effects on privacy. Additionally, a yearly report on any privacy violations and the functioning of the system should be filed by the Government Accountability Office.

Clarifying legal ambiguities and providing businesses with strong liability, FOIA, and regulatory-use protections will allow organizations to share information with little fear of damaging repercussions. This would allow the private sector and government to contribute actively to and learn from others and collaboratively defend U.S. computers and networks.

Past and Proposed Legislation

Multiple pieces of legislation have sought to enable information sharing, and two leading examples deserve a brief discussion. The Cyber Intelligence Sharing and Protection Act (CISPA) has been discussed and passed in the House during the past two Congresses. Over that time however, the bill grew weaker, weakening liability protection to the less-than-adequate "good faith" standard, imposing

unnecessary restrictions on how the government could use this legally and voluntarily exchanged information for combatting crime or enhancing security, as well as privacy mandates that would slow down information sharing, despite the need for this information to be shared rapidly. While CISPA would have encouraged some information sharing, it would have fallen short of fully enabling sharing.[104]

The other proposed measure was the Cybersecurity Information Sharing Act (CISA). CISA had stronger liability protections than CISPA, and more broadly authorized the government to use shared information. On the other hand, it also had some onerous mandates to remove all personally identifiable information from shared information and had less clear regulatory protections.[105]

In 2015, CISA has returned, and two new bills—the National Cybersecurity Protection Advancement Act (NCPAA) and the Protecting Cyber Networks Act (PCNA)—have passed in the House. The PCNA had relatively weak liability protection for sharers, but this issue was fixed in the amendment process.[106] While it has some redundant privacy requirements, it has a good list of authorized uses, making PCNA a strong effort to encourage information sharing. The NCPAA has strong liability protection, but severely restricts the government's use of this information, and also has some duplicative privacy and reporting elements.[107]

Moving Forward on Cybersecurity

While information sharing is far from a silver bullet, it will help improve U.S. cybersecurity. Combined with other policies in the areas of cyber liability and insurance, cyber-supply-chain security, and well-defined rules for limited self-defense, the U.S. can be more secure in cyberspace without government mandates.

Endnotes

101. "Net Losses: Estimating the Global Cost of Cybercrime," McAfee and the Center for Strategic and International Studies, June 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf (accessed May 4, 2015).
102. Paul Rosenzweig, "Cybersecurity Act of 2012: Revised Cyber Bill Still Has Problems," Heritage Foundation *Issue Brief* No. 3675, July 23, 2012, http://www.heritage.org/research/reports/2012/07/cybersecurity-act-of-2012-revised-cyber-bill-still-has-problems.
103. James Gattuso, "Ensuring Cybersecurity: More Red Tape Is Not the Answer," Heritage Foundation *Issue Brief* No. 3626, June 5, 2012, http://www.heritage.org/research/reports/2012/06/cybersecurity-and-red-tape-more-regulations-not-the-answer, and Paul Rosenzweig, "Cybersecurity Act of 2012: Revised Cyber Bill Still Has Problems," Heritage Foundation *Issue Brief* No. 3675, June 23, 2012, http://www.heritage.org/research/reports/2012/07/cybersecurity-act-of-2012-revised-cyber-bill-still-has-problems.
104. Paul Rosenzweig, "CISPA Disappoints in the End," Heritage Foundation *Issue Brief* No. 3594, May 8, 2012, http://www.heritage.org/research/reports/2012/05/cyber-intelligence-sharing-and-protection-act-disappoints-in-the-end.
105. David Inserra, "Senate Cyber Information-Sharing Bill on the Right Track but Improvements Needed," Heritage Foundation *Issue Brief* No. 4269, September 2, 2014, http://www.heritage.org/research/reports/2014/09/senate-cyber-information-sharing-bill-on-the-right-track-but-improvements-needed.
106. David Inserra and Jennifer Guthrie, "House Intelligence Cyber Bill: Amendment Improves Cybersecurity," The Daily Signal, April 22, 2015, http://dailysignal.com/2015/04/22/house-intelligence-cyber-bill-amendment-improves-cybersecurity/.
107. David Inserra and Riley Walters, "House Cyber Information Sharing Bills: Right Approach but Require Fixes," Heritage Foundation *Issue Brief* No. 4382, April 10, 2015, http://www.heritage.org/research/reports/2015/04/house-cyber-information-sharing-bills-right-approach-but-require-fixes.