New Legislation Strengthens Legal Protections for Cybersecurity Information-Sharing

AntitrustConnect Blog
May 1, 2016

Eric McKeown and Emily Storm-Smith (Ice Miller LLP)

Please refer to this post as: Eric McKeown and Emily Storm-Smith, 'New Legislation Strengthens Legal Protections for Cybersecurity Information-Sharing', AntitrustConnect Blog, May 1 2016, http://antitrustconnect.com/2016/05/01/new-legislation-strengthens-legal-protections-for-cybersecurity-information-sharing/

Protecting electronic networks and information systems against cyber-intrusions often requires real-time information sharing among private and governmental entities, but some in the cybersecurity community have expressed concerns in recent years that legal uncertainty has hampered information-sharing efforts. The U.S. Congress recently took steps to address these concerns by passing the Cybersecurity Information Sharing Act of 2015 (CISA or the Act) as part of the 2016 Omnibus Spending Bill. The stated intent of the law's sponsors was to encourage voluntary information-sharing among the federal government and private entities in order to better protect against and respond to data breaches and related cybersecurity incidents. CISA has important implications in a world where hackers seem to keep pace with, and even outstrip, best efforts to secure the information systems that store sensitive personally identifiable information such as employment records and credit card numbers, as well as confidential business information and intellectual property. CISA broadens the legal protections for companies who engage in cybersecurity monitoring and information-sharing activities while requiring compliance with certain measures designed to safeguard individual privacy and civil liberties.

Background

CISA was designed to address uncertainty resulting from the patchwork of various federal and state laws that expose companies and individuals to potential civil and/or criminal penalties for some activities related to cybersecurity. For example, the Electronic Communications Privacy Act (ECPA) imposes liability under certain circumstances for intercepting, accessing, and/or disclosing electronic communications. Likewise, various federal and state laws impose liability based on the disclosure of certain types of personally identifiable information.

CISA addresses key issues regarding liability for monitoring, sharing, or receiving cyber threat information.

Prior to the passage of CISA, some in the data protection and cybersecurity industry expressed concerns regarding the lack of clarity with respect to potential liability for monitoring network and information systems, defending those systems, and/or sharing information about cyber-attacks with the government or other interested parties. Moreover, many in the industry argued that the ability to engage in real-time monitoring and information-sharing is essential to defending against and responding to cyberattacks.

Protection Against Liability for Monitoring and Information-Sharing

CISA addresses key issues regarding liability for monitoring, sharing, or receiving cyber threat information. Under the new law, private entities are broadly protected from liability under any federal or state law, subject to compliance with certain provisions of CISA, for:

- Monitoring their information systems for cybersecurity purposes;
- Implementing certain types of defensive measures to protect their information systems
- Disclosing information pertaining to a cyber-threat to other private entities and the government; and/or
- Receiving such information from other private entities and the government.

These liability protections are subject to an entity’s compliance with, among other

things, the Act's privacy requirements, which are discussed in further detail below. Moreover, CISA defines the type of cyber-threat information that may be shared; companies should carefully consider this definition, as well as the Act's other requirements, in making decisions regarding information-sharing.

These liability protections are subject to an entity's compliance with, among other things, the Act's privacy requirements.

Protection of Information against Disclosure

CISA further incentivizes the sharing of information regarding cyber-attacks by taking steps to alleviate concerns regarding the loss of control over potentially sensitive or valuable business information. To address such concerns, including the risk of public disclosure, CISA classifies all information shared with the government pursuant to the Act as proprietary, exempting such information from disclosure under the Freedom of Information Act (FIOA) or any other federal or state law.

Regulatory/Enforcement Concerns

In addition, CISA provides that cyber-threat information shared with the government may not be used for a regulatory or investigative purpose unrelated to cybersecurity except under certain narrowly defined circumstances, including instances of a specific threat of serious harm to the public or an individual. Thus, the Act mitigates the risk that a company may subject itself to an unrelated regulatory or enforcement action by sharing information related to a cybersecurity threat with the government. Additionally, CISA provides protection against antitrust liability for companies who share information regarding cyber-attacks with other private entities.

Privacy Protections and Requirements

CISA also includes provisions designed to protect the privacy and civil liberties of individuals by limiting the disclosure of personally identifiable information. Before sharing cyber-threat information with any other entity, private or governmental, CISA imposes a duty to review and remove all information, not directly related to the cyber-threat, which includes the personal information of an individual person or could be used to identify a specific individual person. Private entities also may elect to use technical tools to remove such information.

CISA also includes provisions designed to protect the privacy and civil liberties of individuals by limiting the disclosure of personally identifiable information.

Before sharing information with the government or other private entities pursuant to CISA, companies should carefully evaluate their compliance with the privacy requirements of the Act. Forthcoming guidance should aid companies and their counsel in making such determinations. For example, CISA requires the Attorney General and the Department of Homeland Security to issue publicly available guidance identifying types of personal information that are unlikely to be directly related to a cybersecurity threat and may be subject to protection under other privacy laws.

What Next?

CISA provides companies with broad new legal protections for engaging in certain activities designed to strengthen their cybersecurity infrastructure and practices. Moreover, the Act offers private entities some reassurance that cybersecurity information shared with the government is unlikely to be made publicly available or subject the company to unrelated regulatory enforcement action. While the bounds of the CISA have yet to be tested, companies and other organizations likely will look to the Act for guidance in the coming year in designing their own cybersecurity policies and practices.

This article originally appeared in *Intellectual Property & Technology Law Journal*, Vol. 28, No. 5, May 2016.