VENABLE® LLP

Cybersecurity Alert

April 2014

FTC and DOJ Issue Antitrust Policy Statement on Sharing Cybersecurity Information

AUTHORS

Lisa Jose Fales
Robert P. Davis
Jason R. Wool

RELATED PRACTICES

Antitrust
Privacy and Data Security

RELATED INDUSTRIES

Cybersecurity

ARCHIVES

2014 2010 2006
2013 2009 2005
2012 2008 2004
2011 2007

On April 10, 2014, the Federal Trade Commission (FTC) and Department of Justice (DOJ) **issued** a **policy statement** clarifying that the Agencies "do not believe that antitrust is – or should be – a roadblock to legitimate cybersecurity information sharing." But while the policy statement may help to alleviate some concerns that private sector organizations have voiced regarding obstacles to information sharing, it may not go far enough to encourage substantially more. In addition, it does not provide liability protection or a "safe harbor," which has been a primary driver of corporate support for some information sharing legislation to date. Nonetheless, the policy statement could be an important step towards achieving a truly robust cyber-threat sharing ecosystem. In combination with the criteria set out in a 2000 Business Review Letter by DOJ, the policy statement can help entities form the outline of a compliant information sharing program.

Acknowledging that the sharing of information about cybersecurity threats (such as incident or threat reports, indicators, threat signatures, and alerts) can bolster the collective security of networks, the Agencies begin by noting that some private organizations may not be sharing information that could be useful to others out of concern over antitrust enforcement. However, they emphasize that cyber-threat information sharing generally would not raise concerns under the Agencies' "rule of reason" analysis. In applying that analysis, the Agencies focus on "whether the relevant agreement likely harms competition by increasing the ability or incentive profitably to raise price above or reduce output, quality, service, or innovation below what likely would prevail in the absence of the relevant agreement."

The policy statement provides three reasons why cyber-threat information sharing generally would not give the Agencies concern under the rule of reason analysis:

. Threat sharing can improve efficiency and help secure the nation's computer networks. Thus, so long as the purpose for the information sharing is not to participate in a conspiracy to harm competition, the rule of reason analysis would recognize the "valuable" purpose of the information sharing.

. The information being shared is highly technical in nature and is therefore "very different from the sharing of competitively sensitive information such as current or future prices and output or business plans which can raise antitrust concerns."

. In general, cyber-threat information is a "limited category of information" and sharing it is unlikely to harm competition.

Each of these factors is intensely fact-driven, however, which could make it difficult for private sector organizations to rely on the policy statement to share information where the question of whether there may be an adverse impact on competition is a close one. This can be particularly important because an organization's ability to determine whether specific information relates directly, and only, to cybersecurity – especially in real-time – could prove to be challenging.

As a result, private organizations may be hesitant to rely on the policy statement, given that it does not provide a "safe harbor" or liability limitation for instances in which an entity shares information in good faith but unintentionally shares competitively sensitive information. Moreover, antitrust is only one of several areas of concern that many policy makers and businesses hope to see addressed by the federal government. Of particular concern is the role of privacy in information sharing, with the policy debate focusing on the proper balance between privacy safeguards and liability protection for sharing personally identifiable information. The White House is on record in support of "targeted" liability protection for organizations that share information, but some in Congress have voiced support for broader protections to incentivize cyber-threat sharing.

Nonetheless, the policy statement will likely be viewed as a step forward for the information sharing cause, if not the major one that some have been waiting for. As an information sharing bill is rumored to be close to circulation in the Senate Intelligence Committee and the House has already passed the **Cyber Intelligence Sharing and Protection Act**, the policy statement may be a necessary push forward in the effort to pass information sharing legislation.

The **one instance in the past where DOJ reviewed a cybersecurity information sharing program**, the proposal was submitted by the Electric Power Research Institute (EPRI), a non-profit organization focused on the energy industry. **Their proposed program** would share best practices as well as information related "directly to physical and cybersecurity." DOJ determined that as long as the information exchanged was limited as indicated, it "should be sufficient to avoid any threats to competition." Absent legislation, the EPRI letter can serve as guidance to others on how to implement an information sharing program that does not raise antitrust concerns. In the letter, the following program features were explicitly referenced:

- Information sharing of two types: best practices and information related to cyber-vulnerabilities.
    - Best practices include "topics such as methodologies for conducting vulnerability assessments; development of plans to identify, alert, rebuff, and prevent cybersecurity breaches; plans for reconstitution of essential capabilities should an attack succeed; methods for 'stress-testing' the cybersecurity of the energy infrastructure; and activities designed to raise the level of awareness of directors, officers, employees, independent consultants, and others in the energy industry with respect to managing cybersecurity risks."
    - Cyber-vulnerability information could include (1) the status of security technology in existing operating equipment and systems; (2) the results of security testing on specific operating equipment or electronic information or communications systems; (3) solutions to security problems with existing equipment or systems that have been identified or proposed; and (4) concerns that have been identified with such purported solutions.
- The EPRI program, as described, could eventually "include the collaborative reporting, discussion, and analysis of actual real-time cyber-threat and attack information from a variety of sources, including participants, federal and state governments, other infrastructure industries, cybersecurity experts and others, in order to more quickly identify and address in real time any actual cybersecurity threats and attacks on the reliability of the nation's energy supply."
- The program had several features designed to lessen the possibility that its proposed information exchange would have anticompetitive effects:
    - The exchanged information would be "strictly limited in nature" and relate "directly to physical and cyber-security."
    - There would be no "discussion of specific prices for equipment, electronic information or communications systems" or "company-specific competitively sensitive information, i.e., prices, capacity or future plans."
    - The program would not serve as a "conduit for discussions or negotiations between or amongst vendors, manufacturers or security service providers with respect to any participant or group of participants."
    - There would be no recommendations "in favor of or against any product or systems of particular manufacturers or vendors."

These criteria could be used to form the outline of another information sharing program. In addition to these factors, Venable recommends that entities wishing to establish information sharing programs have antitrust compliance programs in place to prevent the sharing of competitively sensitive information, and to the extent possible, have a process for implementing firewalls between those employees with access to "direct" physical and/or cybersecurity information from competitors and those employees involved in pricing, capacity, or output decisions.

For further guidance on developing and implementing an information sharing program, please contact

Venable's experienced team of **Antitrust**, **Cybersecurity**, and **Privacy and Data Security** attorneys.

* * * * * *

Venable LLP offers a broad array of legal services to a variety of different players within the cybersecurity arena. Our attorneys are adept at understanding complex client issues and tapping into the extensive experience of our many practice areas including privacy and data security, e-commerce, intellectual property, antitrust, government contracting, telecommunications, energy, and corporate.

If you have any questions concerning this alert, please contact any of the authors.