

FTC and DOJ Release Guidance on Antitrust Implications of Cybersecurity Information Sharing

April 11, 2014

The Department of Justice's Antitrust Division and the Federal Trade Commission (collectively, the Agencies) on April 10, 2014 released a Policy Statement on private sector sharing of cybersecurity information. The Policy Statement is intended to address some of the concerns raised by industry about barriers to improved private-sector information sharing. The private sector has urged the government to focus on helping industry share information about threats and solutions, rather than embarking on prescriptive regulation. Industry identified areas of risk related to information sharing, including antitrust laws, which arguably chill their freedom to communicate about cyber threats, responses, and capabilities.

In the joint Policy Statement, the Agencies explain that "[s]ome private entities may be hesitant to share cyber threat information with each other, especially competitors, because they have been counseled that sharing of information among competitors may raise antitrust concerns. The Agencies do not believe that antitrust is—or should be—a roadblock to legitimate cybersecurity information sharing."

The statement seeks to explain the Agencies' "analytical framework for information sharing." In sum, because "cyber threat information typically is very technical in nature and very different from the sharing of competitively sensitive information such as current or future prices and output or business plans," the Agencies explain that sharing such threat information "between and among private entities" should not raise traditional antitrust concerns. The Agencies frame this Policy Statement as a continuation of guidance issued many years before,

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law
Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Practice Areas

Government Contracts
Privacy, Cyber & Data Governance
Telecom, Media & Technology

and urge concerned companies to use the Antitrust Division's "business review letter" process to seek further guidance if they have particular concerns.

For purposes of this guidance, the Agencies define "cyber threat information" as "indicators, threat signatures, and alerts" related to a cybersecurity threat. They apply their traditional antitrust analysis to this "limited category of information."

- First, the Agencies explain that "[i]f companies are not sharing such information as part of a conspiracy of the type that typically harms competition, the Agencies' rule of reason analysis would consider the valuable purpose behind the exchange of information" which "is virtually always likely to be done in an effort to protect networks and the information stored on those networks, and to deter cyber attacks."
- Second, the Agencies "would consider the nature of the cyber threat information to be shared among the private parties" which is "very important to the analysis." Because cyber threat information "typically is very technical in nature" the Agencies consider it "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."
- Finally, the Agencies consider the likelihood that sharing would harm competition. "Generally speaking, cyber threat information covers a limited category of information and disseminating information of this nature appears unlikely in the abstract to increase the ability or incentive of participants to raise price or reduce output . . ."

The Agencies' analysis purports to address a narrow type of highly technical information. Drawing on past guidance, the Agencies contrast such information with "discussion of prices for equipment or recommendations in favor of a vendor" and "future product innovation discussions" the sharing of which could be problematic. Thus, the private sector must still be cautious about sharing information about prices, business practices and plans, preferred solutions or vendors, and innovations.

This guidance may partially assuage some of the articulated antitrust concerns, and facilitate industry sharing of certain information. But industry remains concerned about information sharing, and continues to urge "Congress to pass legislation that would provide safe harbor against the risk of frivolous lawsuits, would be exempt from public disclosure, and could not be used by officials to regulate other activities."^[1]

^[1] U.S. Chamber of Commerce: *Agencies' Statement on Antitrust and Cyber Information Sharing is Encouraging*, Friday, April 11, 2014 - 8:30am—Written by Ann M. Beauchesne, available here: <https://www.uschamber.com/blog/agencies-statement-antitrust-and-cyber-information-sharing-encouraging>