DEPARTMENT OF JUSTICE AND FEDERAL TRADE COMMISSION: ANTITRUST POLICY STATEMENT ON SHARING OF CYBERSECURITY INFORMATION

Executive Summary

Cyber threats are becoming increasingly more common, more sophisticated, and more dangerous. One way that private entities may defend against cyber attacks is by sharing technical cyber threat information – such as threat signatures, indicators, and alerts – with each other. Today, much of this sharing is taking place. Some private entities may, however, be hesitant to share cyber threat information with others, especially competitors, because they believe such sharing may raise antitrust issues.

Through this Statement, the Department of Justice's Antitrust Division (the "Division") and the Federal Trade Commission (the "Commission" or "FTC") (collectively, the "Agencies") explain their analytical framework for information sharing and make it clear that they do not believe that antitrust is – or should be – a roadblock to legitimate cybersecurity information sharing. 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.

Specific guidance in the context of cybersecurity information was previously provided by the Division's October 2000 business review letter to the Electric Power Research Institute, Inc. (EPRI). The Division confirmed that it had no intention to initiate an enforcement action against EPRI's proposal to exchange certain cybersecurity information, including exchanging actual real-time cyber threat and attack information. While this guidance is now over a decade old, it remains the Agencies' current analysis that properly designed sharing of cybersecurity threat information is not likely to raise antitrust concerns.

indicators,[5] threat signatures,[6] and alerts[7] (collectively, “cyber threat information”) among these entities has the potential to

mentioned above is highly unlikely to lead to a reduction in competition and, consequently, would not be likely to raise antitrust concerns. To decrease uncertainty regarding the Agencies' analysis of this type of information sharing, the Agencies are issuing this Statement to describe how they analyze cyber threat information sharing.

2. An

competitive coordination among competitors.[12] The joint DOJ/FTC Antitrust Guidelines for Collaborations Among Competitors provide a good overview of how the Agencies analyze information sharing as a general matter.[13]

First, these

> The [Antitrust] Agencies recognize that the sharing of information among competitors may be procompetitive and is often reasonably necessary to achieve the procompetitive benefits of certain collaborations … Nevertheless, in some cases, the sharing of information related to a market in which the collaboration operates or in which the participants are actual or potential competitors may increase the likelihood of collusion on matters such as price, output, or other competitively sensitive variables. The competitive concern depends on the nature of the information shared. Other things being equal, the sharing of information relating to price, output, costs, or strategic planning is more likely to raise competitive concern than the sharing of information relating to less competitively sensitive variables. Similarly, other things being equal, the sharing of information on current operating and future business plans is more likely to raise concerns than the sharing of historical information.[15]

Within this framework, when evaluating an exchange of information the Agencies consider the extent to which competitively sensitive information likely would be disclosed to competitors. Antitrust risk is lower when the shared information is less competitively sensitive and unlikely to lead to a lessening of competition; thus the nature and detail of the information disclosed and the context in which information is shared are highly relevant. Additionally, it is less likely that the information sharing arrangements will facilitate collusion on competitively sensitive variables if appropriate safeguards governing information sharing are implemented to prevent or minimize such disclosure.

b. Antitrust Analysis of Cyber Threat Information Sharing

The analytical framework outlined above applies irrespective of industry. Below we apply that analysis with respect to the exchange of cyber threat information.

First, sharing of cyber threat information can improve efficiency and help secure our nation's networks of information and resources. It appears that this sharing 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. If companies are not sharing such

[15] Id. at 15. See also United States v. United States Gypsum, 438 U.S. 422 (1978), examining whether the information exchanged has a legitimate purpose, or is more likely to be used for collusive purposes.

information as part of a conspiracy of the type that typically harms competition, the Agencies'

quality, service, or innovation. However, this type of analysis is intensely fact-driven. In the one instance in which the Division had occasion to review a cybersecurity information sharing arrangement, it concluded that antitrust concerns did not arise. This was in a favorable business review letter that the Division issued in 2000 to EPRI, a nonprofit organization "committed to providing and disseminating science and technology-based solutions to energy industry problems."[18] The business review involved a proposal to share information to improve physical and cyber security. EPRI had developed an Enterprise Infrastructure Security (EIS) program to assist the various energy industries in addressing security risks raised by the increased interconnection, interdependence, and computerization of the energy sector, its suppliers, and customers.

EPRI proposed exchanging two types of information: best practices and information related to cybersecurity vulnerabilities. EPRI further noted that the program eventually might include a discussion and analysis of actual real time cyber threat and attack information from a variety of sources, including participants, federal and state

proposed information exchanges result in more efficient means of reducing cybersecurity costs, and such savings redound to the benefit of consumers, the information exchanges could be procompetitive in effect."[19]

Although the nature, complexity, and number of threats have changed since the Division issued the EPRI letter, the legal analysis in the letter remains very current.[20] Thus, the Agencies' guidance establishes that properly designed sharing of cyber threat information should not raise antitrust concerns.[21]

[19] Id. at 3-4. See also Letter from Joel I. Klein, Assistant Att'y Gen., Antitrust Div., U.S. Dep't of Justice, to Robert B. Bell, Partner, Wiley, Rein & Fielding (July 1, 1998), available at http://www.justice.gov/atr/public/busreview/1824.htm (exchange of information including methods of remediating Year 2000 problems); Letter from Joel I. Klein, Assistant Att'y Gen., Antitrust Div., U.S. Dep't of Justice, to Jerry J. Jasinowski, President, Nat'l Assoc. of Mfrs. (Aug. 14, 1998), available at http://www.justice.gov/atr/public/busreview/1877.htm (exchange of information including methods of remediating Year 2000 problems, including promoting bilateral exchanges between Association members) (The Department noted it would be concerned if parties, under the guise of a Year 2000 remedial program, exchanged price or other competitively-sensitive information, agreed not to compete for particular business, agreed not to deal with certain suppliers or entered into other anticompetitive agreements); Letter from J. Mark Gidley, Acting Assistant Att'y Gen., Antitrust Div., U.S. Dep't of Justice, to Stuart M. Pape, Partner, Patton, Boggs & Blow (Jan. 14, 1993), available at http://www.justice.gov/atr/public/busreview/211550 htm (in issuing a favorable review the Division noted that the "information to be exchanged among the venture participants, however, will be solely of a technical nature….").

[20] See, e.g., Renata B. Hesse, Deputy Assistant Att'y Gen., Antitrust Div., U.S. Dep't of Justice, At the Intersection of Antitrust & High-Tech: Opportunities for Constructive Engagement, Remarks as Prepared for the Conference on Competition and IP Policy in High-Technology Industries at 10-11 (Jan. 22, 2014), available at http://www.justice.gov/atr/public/speeches/303152.pdf. ("While this [EPRI] guidance is now over a decade old, it remains the Antitrust Division's current analysis that properly designed sharing of cyber-security threat information is not likely to raise antitrust concerns.").

[21] Of course, if an information sharing arrangement is being used as a cover to fix prices, allocate markets, or otherwise limit competition, antitrust issues could arise.