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.

1. Overview of Cybersecurity and Information Sharing

The Agencies share the President's view that "cyber threat is one of the most serious economic and national security challenges we face as a nation"[1] and are committed to doing all they can to improve the safety of our nation's networks.[2] Our modern economy and national security depend on a secure cyberspace. Core features of our nation's cybersecurity strategy are to improve our resilience to cyber incidents and to reduce and defend against cyber threats. One way to make progress on these fronts is by increasing cyber threat information sharing between the government and industry, and among industry participants. In his February 2013 Executive Order, the President highlighted the important role the government can play in sharing information with U.S. private sector entities, while ensuring that privacy and civil liberties protections are in place.[3] Another important component of securing our IT infrastructure is through the sharing of cybersecurity information between and among private entities. In particular, the sharing of information about cybersecurity threats,[4] such as incident or threat reports,

---

[1] *Cyber Security*, THE WHITE HOUSE, *available at* http://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

[2] Through its Computer Crime and Intellectual Property Section, the Department of Justice (the "Department" or "DOJ") has trained prosecutors to focus on investigating and prosecuting cybercrime and intellectual property cases in each of the nation's 94 federal districts. The National Security Division's (NSD) National Security Cyber Specialists (NSCS) Network brings together the Department's full range of expertise on national security-related cyber matters, drawing on experts from NSD, the U.S. Attorney's Offices, and other Department components. The Department has emphasized using all of its legal tools to disrupt and dismantle criminal cyber infrastructure, such as botnets, and to arrest those responsible for building and operating such infrastructure for criminal purposes.

[3] Executive Order: Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[4] In its 2011 legislative proposal, the Administration defined a cybersecurity threat as "any action that may result in unauthorized access to, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information stored on or transiting an information system, or unauthorized exfiltration of information stored on or transiting an information system." Law Enforcement Provisions Related to Computer Security § 242(8) (2011), available at

indicators,[5] threat signatures,[6] and alerts[7] (collectively, "cyber threat information") among these entities has the potential to greatly improve the safety of our systems.

Today, some private-to-private cyber threat information sharing is taking place, both informally and through formal exchanges or agreements, such as the many sector-specific Information Sharing Analysis Centers (ISACs) that have been established to advance the physical and cybersecurity of critical infrastructures.[8] Sharing can take many forms – it may be unstructured or very structured, human-to-human or automated, or somewhere in between. There are a number of benefits that derive from these arrangements – foremost, they increase the security, availability, integrity, and efficiency of our information systems. This, in turn, leads to a more secure and productive nation.

Some 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. While it is true that certain information sharing agreements among competitors can raise competitive concerns, sharing of the cyber threat information

---

http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf.

[5] Indicators may include, for example, file hashes, computer code, malicious URLs, source email addresses, and technical characteristics of malware (*e.g.*, "a pdf file of a certain size attached").

[6] Threat signatures are the characteristics of specific cyber threats that may be used (often by automated systems) to identify, detect, and/or interdict them. Typically, multiple indicators are used to generate a threat signature.

[7] An alert is intended to provide timely notification of security threats or activity. *See, e.g.*, 2014 Alerts, UNITED STATES COMPUTER EMERGENCY READINESS TEAM, *available at* http://www.us-cert.gov/ncas/alerts.

[8] *See, e.g., About Us: Information Sharing and Analysis Centers (ISACs)*, NATIONAL COUNCIL OF ISACS, *available at* http://www.isaccouncil.org/aboutus.html.

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. Antitrust Analysis of Information Sharing Agreements

a. General Overview

The Agencies' Antitrust Guidelines,[9] business review letters,[10] and advisory opinions[11] explain the analytical framework for information sharing and the competition issues that may arise with information exchanges generally. The Agencies' primary concern in this context is that the sharing of competitively sensitive information – such as recent, current, and future prices, cost data, or output levels – may facilitate price or other

---

[9] U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST GUIDELINES FOR COLLABORATIONS AMONG COMPETITORS (2000), *available at* http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf [hereinafter COMPETITOR COLLABORATION GUIDELINES]; U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, STATEMENTS OF ANTITRUST ENFORCEMENT POLICY IN HEALTHCARE (1996), *available at* http://www.justice.gov/atr/public/guidelines/0000.htm [hereinafter HEALTHCARE STATEMENTS]; U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST GUIDELINES FOR THE LICENSING OF INTELLECTUAL PROPERTY 13 (1995), *available at* http://www.justice.gov/atr/public/guidelines/0558.htm [hereinafter IP LICENSING GUIDELINES].

[10] Individuals who are concerned about the legality of future business activities under the antitrust laws can formally request that the Division issue a statement of its present enforcement intentions. 28 C.F.R. §50.6 (2010). If firms are concerned about a specific proposed program, they may choose to utilize the Division's business review process. Business review letters allow the Division to take these general principles and provide prospective guidance to specific proposals. The Division is committed to resolving the request as expeditiously as possible so that it does not get in the way of legitimate collaborations. *See Business Reviews*, ANTITRUST DIV., U.S. DEP'T OF JUSTICE, *available at* http://www.justice.gov/atr/public/busreview/index.html.

[11] The Commission's Rules of Practice provide that the Commission or its staff, in appropriate circumstances, may offer industry guidance in the form of an advisory opinion. *See* 16 C.F.R. §§ 1.1-1.4.; *see also* http://www.ftc.gov/tips-advice/competition-guidance/competition-advisory-opinions. FTC staff recently issued an advisory opinion to the U.S. Money Transmitters regarding an information exchange program advising that the program was unlikely to harm competition and may enhance consumer protection goals. Letter from Michael J. Bloom, Asst. Dir., Bureau of Competition, Fed. Trade Comm'n, to Ezra C. Levine, Senior Of Counsel, Morrison & Foerster LLP (Sept. 4, 2013), *available at* http://www.ftc.gov/policy/advisory-opinions/money-services-round-table.

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 Guidelines note that the antitrust agencies will typically examine information sharing agreements under a rule of reason analysis, which considers the overall competitive effect of an agreement. "Rule of reason analysis focuses on the state of competition with, as compared to without, the relevant agreement. The central question is 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."[14] In some cases, the nature of the agreement may demonstrate the lack of competitive harm. In examining the nature of the relevant agreement, the Agencies take into account the business purposes for the agreement. If competitive harm seems likely, the Agencies will analyze the agreement in more depth to evaluate countervailing efficiencies.

The Competitor Collaboration Guidelines further explain the Agencies' analysis:

---

[12] COMPETITOR COLLABORATION GUIDELINES, *supra* note 9, at 21; HEALTHCARE STATEMENTS, *supra* note 9, at 64 ("Exchanges of future prices … are very likely to be considered anticompetitive); IP LICENSING GUIDELINES, *supra* note 9, at 13 ("The risk [that a joint venture would adversely affect competition] … would be increased to the extent that, for example, the joint venture facilitates the exchange among the parties of competitively sensitive information relating to the [] markets in which the parties currently compete, or facilitates the coordination in such markets.").

[13] COMPETITOR COLLABORATION GUIDELINES, *supra* note 9; *see also* HEALTH CARE STATEMENTS, *supra* note 9. (These include guidelines for the dissemination of price and cost data, as well as non-fee related information, among health care providers and have been applied outside of the Health Care context); Case law also recognizes that gathering and disseminating information can be procompetitive. *See United States v. United States Gypsum Co.*, 438 U.S. 422, 441 n.16 (1978) ("The exchange of price data and other information among competitors does not invariably have anticompetitive effects; indeed such practices can in certain circumstances increase economic efficiency and render markets more, rather than less, competitive.").

[14] COMPETITOR COLLABORATION GUIDELINES, *supra* note 9, at 4.

> 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 Co.*, 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' rule of reason analysis would consider the valuable purpose behind the exchange of information.

Second, the Agencies would consider the nature of the cyber threat information to be shared among the private parties. The nature of the information being shared is very important to the analysis. Cyber threat information typically is very technical in nature. For example, one of the most common methods of identifying malware (*e.g.*, a virus, worm, etc.) is through signature detection. A threat signature is like a digital fingerprint; it is a unique string of bits or data that uniquely identifies a specific threat. Signature-based detection involves searching for known patterns of data. Sharing a signature for a previously unknown threat will enable the recipient to take action to prevent, detect, or contain an attack. Similarly, knowing the source IP address or target port of a Denial of Service (DOS) attack[16] may enable one to take protective measures against such an attack by blocking illegitimate traffic. The sharing of this type of information is 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 would consider whether the exchange is likely to harm competition. Generally speaking, cyber threat information covers a limited category of information[17] 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,

[16] A DOS attack involves flooding a targeted system with incoming, useless traffic with the goal of making the attacked network unavailable to its intended users.

[17] In addition, the Agencies understand that many companies have antitrust compliance programs in place to prevent the sharing of competitively sensitive information.

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 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. All information exchanged would relate directly to physical and cybersecurity, and there would be no discussion of prices for equipment or recommendations in favor of a vendor. The Division concluded that "[a]s long as the information exchanged is limited…to physical and cybersecurity issues, the proposed interdictions on price, purchasing and future product innovation discussions should be sufficient to avoid any threats to competition. Indeed, to the extent that the

[18] Letter from Joel I. Klein, Assistant Att'y Gen., Antitrust Div., U.S. Dep't of Justice, to Barbara Greenspan, Assoc. Gen. Counsel, Electric Power Research Inst. (Oct. 2, 2000), *available at* http://www.justice.gov/atr/public/busreview/6614.htm.

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.