Sharing Cyber Threat Information: A Legal Perspective

By David Navetta and Utsav Mathur

This article discusses recent efforts by the US federal government to allow for more cyber-threat information sharing within industries and potential legal risks for organizations participating in information exchanges.

Abstract

This article discusses recent efforts by the US federal government to allow for more information sharing concerning cyber threats and data-security incidents within industries, including a Department of Justice and Federal Trade Commission policy statement on the antitrust implications of sharing cybersecurity information between entities in an industry. The article also discusses potential legal risks for organizations participating in or relying on data-security information exchanges.

In 2014 a seemingly endless rash of highly publicized data breaches and cyber attacks stunned not only those in the affected industries but also the public at large. It is not surprising then that companies are taking notice of this growing threat and are working to develop effective defense strategies. Yet, no defense strategy can be truly effective without accurate threat information. And that information is best obtained from the companies that have recently experienced an attack.

Consequently, sharing cyber-threat information between companies within an industry is considered to be one of the key strategies in combating cyber attacks. The White House and federal agencies are chief among the proponents of cyber-threat information sharing; they have made clear that sharing threat information among industry participants is critical to effective cybersecurity.[1]

While information sharing between the private sector and government is not new,[2] information sharing within an industry raises a whole host of new concerns. For instance, information sharing between market competitors may provoke the ire of US and other antitrust enforcers. Beyond the antitrust worries, there are the obvious practical concerns: is the information being shared accurate and reliable, and can the information act as a road map for bad actors to penetrate existing defenses. So, does information sharing create more problems than it solves?

Federal agencies signal that legitimate cyber information sharing within appropriate parameters will not trigger antitrust alarms

Recognizing that the specter of antitrust prosecution may hinder crucial cybersecurity information-sharing efforts, the agencies tasked with enforcing US antitrust laws—the US Department of Justice and the Federal Trade Commission ("Agencies")—jointly issued a Policy Statement in April 2014 addressing that very point.[3]

In their statement, the Agencies explained that the antitrust laws do not, and should not, attach liability to legitimate cybersecurity information sharing, as long as the sharing does not encroach on competitively sensitive information related to price, cost, or output. The Agencies reasoned that cyber-threat information is typically "very technical in nature

1 Michael Daniel, *Strengthening Our Cyber Community*, The White House Blog (Sept. 19, 2014, 3:17 PM), http://www.whitehouse.gov/blog/2014/09/19/strengthening-our-cyber-community; National Institute of Standards and Technology, "Notice: Experience With the Framework for Improving Critical Infrastructure Cybersecurity" (Aug. 26, 2014), https://www.federalregister.gov/articles/2014/08/26/2014-20315/experience-with-the-framework-for-improving-critical-infrastructure-cybersecurity (last visited on Dec. 4, 2014).

2 In 1998 President Clinton signed PDD-63 which resulted in the creation of Information Sharing and Analysis Centers in partnership with the private sector. It also established organizations to provide central coordination including the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, the Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, and the National Infrastructure Assurance Council.

3 Department of Justice & Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information (Apr. 10, 2014), available at http://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf.

and very different from the sharing of competitively sensitive information," and sharing that information would appear to benefit rather than harm competition.[4] The Agencies warned, however, that antitrust analysis was "intensely fact-driven,"[5] conveying that their statement was meant to guide but not bind antitrust enforcement.

The same day the Agencies issued their statement, the White House Cybersecurity Director weighed in,[6] approving the Agencies' guidance as "so important" to cybersecurity efforts and reaffirming the administration's commitment to facilitate information sharing among governmental and private entities—as was highlighted prominently in the president's February 2013 Executive Order 13636.[7] Recent statements from the White House, although not addressing antitrust liability specifically, have continued to stress the importance of information sharing and cooperation among the public and private sectors.[8]

Antitrust concerns in the cybersecurity context, however, have not been laid to rest. A few months after the policy statement was released, the Center for the Study of the Presidency and Congress, a nonprofit policy and education organization, published a report that again raised the issue of cybersecurity information sharing and antitrust liability.[9] That report reflected a yearlong project and series of roundtables that brought together representatives from the Executive Branch, Congress, and the private sector to discuss threats to the US electric grid, including threats of cyber attack. Although recognizing the Agencies' policy statement as a "step in the right direction," the report warned that "it still does not go far enough," because "[a] verbal statement simply does not have the force that legislation or even an executive order has, and that kind of definitive law is the only way to fully put liability concerns to bed."[10] Those liability concerns, particularly in the antitrust arena, the report explained, may inhibit potential industry expansion of information sharing, identified as beneficial and necessary to the war against cyberattacks.[11] The report called for "continued assurances…so that such information exchange is not viewed as collusion by antitrust regulators."[12] Although there is some concern that a mere policy statement does not go far enough, recent DOJ action further suggests that the agency does not want antitrust concerns to stifle legitimate cyber information sharing.

4 Ibid.

5 Ibid. at 8.

6 Michael Daniel, *Getting Serious about Information Sharing for Cybersecurity*, The White House Blog (Apr. 10, 2014, 1:45 PM), http://www.whitehouse.gov/blog/2014/04/10/getting-serious-about-information-sharing-cybersecurity.

7 Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013), available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

8 Michael Daniel, *supra* note 1.

9 Center for the Study of the Presidency & Congress, *Securing the U.S. Electrical Grid: Understanding the Threats to the Most Critical of Critical Infrastructure, While Securing a Changing Grid* (1st ed. July 15, 2014), https://www.thepresidency.org/publications/securing-us-electrical-grid.

10 Ibid. at 98-99.

11 Ibid. 131.

12 Ibid. 61.

Cyber policy at work: DOJ indicates no present intent to challenge information exchange on antitrust grounds

On October 2, 2014, in response to a business review request, the DOJ announced that it will not challenge a proposed cyber intelligence data-sharing platform.[13] Not long after the Agencies issued the above-discussed policy statement, CyberPoint International LLC, a private entity offering cybersecurity services, formally requested a "business review letter"[14] from the DOJ's Antitrust Division to assess CyberPoint's proposed cyber-threat information sharing platform.[15] The platform, called True Security Through Anonymous Reporting or TruSTAR, will permit its members anonymously to share cyber-threat information and mitigation techniques. Members will be free to use the data posted on the platform to enhance their own cyber preparedness.

Traditionally, information exchanges like TruSTAR or proposals "to collect and disseminate business information,"[16] have raised antitrust red flags. The DOJ's business review letter placated those concerns for CyberPoint by stating that it has "no present intention to challenge" the TruSTAR platform under US antitrust laws.[17] The DOJ's review did not stray from the April 2014 policy statement.[18] Indeed, in a press release accompanying the October 2 TruSTAR letter, the DOJ cited the policy statement to underscore the importance of collaboration, even between market competitors, in combating 21st century cyber threats.[19] As previewed in the policy statement, the DOJ applied "rule of reason" analysis to the TruSTAR platform, focusing on the central question of "whether the [platform] 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 [platform]."[20] Three primary factors drove the analysis:

- **The business purpose and nature of the platform**: TruSTAR sought to "share cybersecurity information among private entities to protect networks and deter cyber attacks."

13 Letter from The Hon. William J. Baer, Office of the Assistant Att'y Gen., U.S. Dep't of Justice, Antitrust Division, to Steven A. Bowers, Counsel for CyberPoint International LLC, at 1 n.2 (Oct. 2, 2014), available at http://www.justice.gov/atr/public/busreview/309071.pdf.

14 Under 28 C.F.R. § 50.6, a business review letter has "no application to any party which does not join in the request therefor."

15 Letter from Steven A. Bowers to The Hon. William J. Baer (July 1, 2014), available at http://www.justice.gov/atr/public/busreview/request-letters/309073.pdf.

16 *See* 28 C.F.R. § 50.7 Consent judgments in actions to enjoin discharges of pollutants, available at http://www.justice.gov/atr/public/busreview/201659a.htm.

17 Letter from The Hon. William J. Baer to Steven A. Bowers (Oct. 2, 2014), available at http://www.justice.gov/atr/public/busreview/309071.pdf.

18 *Dept. of Justice & Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information* (Apr. 10, 2014), available at http://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf.

19 Press Release, Dept. of Justice, Department of Justice Will Not Challenge Proposed Cyber Intelligence Data-Sharing Platform (Oct. 3, 2014) http://www.justice.gov/atr/public/press_releases/2014/309067.pdf.

20 Letter from The Hon. William J. Baer to Steven A. Bowers (Oct. 2, 2014), available at http://www.justice.gov/atr/public/busreview/309071.pdf.

- **The type of information shared**: Platform members would anonymously post highly technical cyber data that "is unlikely to facilitate tacit or explicit price or other competitive coordination among competitors."
- **The safeguards implemented to minimize the risk of disclosure of competitively sensitive information**: No competitively sensitive information about recent, current, and future prices, cost data, output levels, or capacity will be exchanged through the platform. In fact, as a condition to membership, all platform users would have to commit not to share competitively sensitive information.

This statement should provide further reassurance that cyber information sharing will not incur the scrutiny of US antitrust enforcement agencies if undertaken in an appropriate manner. Rather it appears that the federal government genuinely wants to encourage private sector information sharing. As long as the information sharing does not encroach on competitively sensitive information related to price, cost, or output, market participants' risk of antitrust prosecution should be tolerably low. That said, antitrust enforcement is not the only risk that market participants face in sharing cyber threat information.

Beyond antitrust, cyber information sharing raises unique legal and practical concerns

Sharing private threat information, even on an anonymous information exchange, can pose legal and practical risks. For instance, statements made on an information exchange, even anonymous ones, can be traced back to a corporate employee and can be used against the corporation in litigation. Additionally, hackers could scour the information exchanges to identify common defense strategies and develop countermeasures. Worse still, a hacker may be able to discover a company's cyber weaknesses based on the questions and comments raised by its employee posters. To borrow from a long discarded warning, a loose lip on the information exchange could end up sinking the corporate ship. Some of the specific risks that market participants face are discussed below.

Corporate disclosures

The Securities and Exchange Commission, as the foremost regulator of public companies, has broad jurisdictional reach and enforcement powers. The SEC has issued guidance instructing companies to disclose their cyber risks to investors. These disclosures are carefully crafted to ensure compliance with SEC expectations. The problem arises when corporate employees are discussing the company's cyber risks on an information exchange or providing security information to an exchange without regard to the investor disclosures the company has made. Information provided to those exchanges could lead to SEC enforcement and could be used in shareholder litigation if they are inconsistent with the formal risk disclosures and violate securities laws.

Industry standards

Generally, in assessing whether a company acted reasonably in protecting consumer or other sensitive data (e.g., for purposes of adjudicating negligence claims and otherwise), courts and regulators may judge the company's actions against those of other industry participants (i.e., the industry standard). Industry-focused cyber information exchanges may help participants in a particular industry ascertain generally accepted industry standards around information security. However, the failure to participate in an exchange and to match the practices reflected in the exchange could be used by plaintiffs to establish that an organization has not met the appropriate standard of care for protecting information or systems. Moreover, poorly designed exchanges that fail to distinguish between generally accepted industry standards and aspirational standards that go beyond the industry norm could lead to confusion and the imposition of standards in a legal context that are too high.

Misinformation, incomplete or inaccurate information

Corporate actors will need to carefully vet all information learned through private exchanges, especially if the information is posted anonymously. Bad actors could plant disinformation. For instance, a bad actor could propose a defense strategy with a built-in back door that could be exploited at a later date. Beyond malicious actors, information exchanges that are poorly organized, not standardized, not updated, or use incomplete or inaccurate information can lead participants astray when it comes to managing their data security and, ultimately, legal risk.

Conclusion

These are only some of the concerns that companies will need to navigate as they engage in private threat information sharing. Additional concerns will surely come to light as more industry participants engage in this process. That said, the message here is not that companies should avoid information sharing, just that they should proceed cautiously and should think through and plan for predictable pitfalls.

About the Authors

David Navetta, Esq., CIPP/US, is the US co-chair of Norton Rose Fulbright's Data Protection, Privacy, and Access to Information practice group. David focuses on technology, privacy, information security and intellectual property law. David has spoken and written frequently concerning technology, privacy, and data security legal issues and can be reached at david.navetta@nortonrosefulbright.com

Utsav Mathur, Esq., is an associate in Norton Rose Fulbright's Data Protection, Privacy, and Access to Information practice group. He serves clients in the banking, retail, energy and shipping industries.