Law360

April 16, 2014

Antitrust Guidance On Cybersecurity Reaffirms Old Approach

by Jamillia Padua Ferris and Paul M. Tiao

On April 10, Deputy Attorney General James Cole, White House senior adviser Rand Beers, the head of the U.S. Department of Justice Antitrust Division and the chairwoman of the Federal Trade Commission announced the release of the antitrust agencies' "Antitrust Policy Statement on Sharing of Cybersecurity Information." This statement — consistent with prior DOJ guidance — makes clear that the FTC and DOJ do not view the antitrust laws as a barrier to sharing cybersecurity information, even among competitors.

The sharing of operational information is a critical element in the fight against cyberthreats. Every day, government agencies and private companies face a wide variety of cyberattacks, including hacking efforts to circumvent logical security mechanisms, exploitation based on weak or stolen credentials, malicious software in the form of spyware, keyloggers, RAM scrapers, and backdoors, strategic Web compromises such as watering holes, and social engineering in the form of phishing and SMishing, to name just a few.

Threat actors constantly change their tactics in order to circumvent the efforts of network defense professionals, frequently targeting large numbers of entities in search of vulnerabilities that they can exploit. In this environment, the sharing of current intelligence about cyberthreats and vulnerabilities between private entities and between the government and the private sector is essential.

Information security professionals rely on timely cybersecurity information to keep up with the current attack vectors of hostile nation-states, hacktivists, criminal organizations and terrorists. Through robust information-sharing about the latest IP addresses, URLs, email addresses, malware, social engineering schemes and other tools or tactics in use by hackers, network security professionals significantly increase their ability to block or mitigate the effects of a cyberattack.

The administration recognizes the importance of sharing information about cyberthreats and vulnerabilities. The president's 2013 "Executive Order on Improving Critical Infrastructure" requires certain agencies to share classified and unclassified cyberthreat information with targeted companies. And, the U.S. Department of Homeland Security, the Federal Bureau of Investigation and the U.S. Department of Energy are rapidly expanding programs designed to facilitate the bidirectional sharing of technical cybersecurity information between the government and the private sector.

However, concerns about possible reputational harm, litigation or regulatory action have hindered effective information-sharing. These concerns take a variety of forms but antitrust risk has proven to be a significant issue. In a testament to the ubiquity (and, arguably, success) of antitrust compliance efforts, companies have been reluctant to share cyberthreat information with their competitors out of fear of the consequences of violating the antitrust laws. Having been well counseled by their lawyers about the substantial criminal and civil penalties resulting from antitrust violations, companies have expressed concern about engaging in activities that appear to run contrary to that guidance, even in furtherance of the laudable and shared goal of protecting the nation's information technology infrastructure.

Congress has attempted to address these concerns through legislation intended to remove perceived statutory obstacles to information-sharing. For example, the Cyber Intelligence Sharing and Protection Act of 2013, the National Cybersecurity and Critical Infrastructure Protection Act of 2013 and the Cybersecurity Act of 2012 all would authorize private entities to share cyberthreat information with other private entities and with the government "notwithstanding any other provision of law." This provision would effectively address companies' antitrust concerns, but it does not appear likely that cybersecurity legislation will become law any time soon. In this context, the "Antitrust Policy Statement on Sharing of Cybersecurity Information" is significant. It responds to industry's concerns by clearly establishing that properly designed and executed cyberthreat information-sharing does not raise antitrust concerns.

The analysis underlying the policy statement is not new. The antitrust agencies have long recognized that information-sharing can be necessary to achieve pro-competitive benefits and economic efficiencies in a variety of contexts. For that reason, the antitrust agencies have interpreted the antitrust laws as permitting such sharing if it is unlikely to lead to competitive harm.

Information-sharing activities generally are analyzed under the flexible rule of reason standard, which considers the overall effect of an agreement. This approach considers the business purpose of an agreement and the type of information shared. Certain information exchanges, such as those involving price, output, costs or future plans, are more likely to raise competition concerns than sharing less competitively sensitive information.

Consistent with this standard, the "Antitrust Policy Statement on Sharing of Cybersecurity Information" acknowledges that as a general matter the sharing of cyberthreat information has the valuable purpose of protecting IT networks, and it involves only a narrow category of information. In addition, the policy statement cites guidance, now more than a decade old, in which the DOJ concluded that information-sharing in the context of cybersecurity threats was appropriate in certain circumstances.

In 2000, the Electric Power Research Institute (EPRI) requested that the Antitrust Division issue a business review letter that would provide EPRI with the DOJ's enforcement intent with respect to EPRI's proposed Enterprise Infrastructure Program (the "EIS Program") — a collaborative effort among energy industry participants designed to respond to cybersecurity threats.[1]

A primary component of the EIS Program was facilitating information exchanges among competing electric power, natural gas and petrochemical companies. This included the sharing of: (1) energy industry-specific "best practices" for cybersecurity programs; (2) information relating to cybersecurity vulnerabilities in operating equipment, electronic information and communications systems; (3) real-time reporting and analysis of cyberthreats and attacks; and (4) potentially, desired electronic security requirements and features in the form of commonly accepted functional security specifications for future equipment and systems.

The Antitrust Division responded favorably to the EPRI proposal, concluding that the information exchange would not restrict competition. Relevant to the analysis were certain measures that lessened the possibility that the proposed information exchange would have anti-competitive effects, including:

- Open membership for industry members;
- Limiting information exchanged to physical and cybersecurity information;
- Avoiding discussion about specific prices for equipment, electronic information or communications systems and company-specific, competitively sensitive information (i.e., prices, capacity, future plans);
- Not recommending any manufacturer's products or systems; and
- Not allowing the EIS Program to serve as a conduit for discussions or negotiations between or among vendors, manufacturers or security service providers.[2]

Earlier this year Antitrust Division Deputy Assistant Attorney General Renata Hesse cited this guidance favorably in a published speech delivered at Stanford. The additional release of the policy statement makes clear that the EPRI business review both reflects antitrust agencies' view of cybersecurity information exchanges and is applicable to other industries as well.

Of course, the policy statement is not a free pass for companies to engage in unlawful information-sharing. Whether or not any particular cybersecurity information-sharing program violates the antitrust laws will continue to depend on the specifics of the collaboration, and companies should always have antitrust safeguards in place. However, as Assistant Attorney General Bill Baer stated last week, "This is an antitrust no-brainer … . [A]s long as companies don't discuss competitive information such as pricing and output when they are sharing cybersecurity information, they're ok."

Jamillia Padua Ferris and Paul Tiao are partners in Hunton & Williams' Washington, D.C., office.

[1] See Letter from Electric Power Research Inst. (June 2, 2000), available at http://www.justice.gov/atr/public/busreview/request-letters/302319.pdf. The Antitrust Division's business review procedure provides a method for businesses to get the agency's view of, and enforcement intent with respect to, proposed business conduct. See generally, US Dept. of Justice, Antitrust Division, Introduction to Antitrust Division Business Reviews, available at http://www.justice.gov/atr/public/busreview/276833.pdf.

[2] Id.