crowell moring

CLIENT ALERT

DOJ and FTC State that Antitrust is Not a Roadblock to Cybersecurity Information Sharing

Apr.12.2014

The Department of Justice and the Federal Trade Commission on April 10 issued *Antitrust Policy Statement on Sharing of Cybersecurity Information*, a joint policy statement that provides critical infrastructure industries the clarity they need to share cybersecurity information among themselves to combat cyber threats without violating the antitrust laws those agencies enforce. The agencies note that "properly designed cyber threat information sharing is not likely to raise antitrust concerns and can help secure the nation's networks of information and resources." The benefits of sharing this highly technical information are significant: sharing increases the security, availability, integrity, and efficiency of information systems, which in turn, leads to a more secure and productive nation. The agencies make clear that they "do not believe that antitrust is—or should be—a roadblock to legitimate cybersecurity information sharing." This policy statement is meant to provide more certainty to the concerns private companies have raised as the threats to our nation's infrastructure and information systems increase in number and sophistication.

The ABA noted the companies' antitrust concerns with respect to this information sharing last November. In its publication, *A Playbook for Cyber Events,* the Standing Committee on Law and National Security stated that "antitrust concerns have triggered suspicion about close coordination among corporate competitors including discussions of cybersecurity information sharing." The Committee went on to state that it would be appropriate for companies collaborating on cybersecurity information sharing to address antitrust concerns, while highlighting that DOJ's guidance and discussions with former Antitrust Division attorneys support the notion that antitrust is not a roadblock to properly conducted cyber-related information sharing.

Recent Happenings in APRM
June 2014

- Supreme Court Permits Lanham Act Challenge to Beverage Label Regulated by the FDA
- Highlights from ACI's 2014 Consumer Products Regulatory & Litigation Program
- Updates on the Accessibility Front
- Substantial Harm to Consumer Product Sector Expected Under Proposed Prop 65 'Reforms'
- New Opportunity to Influence CPSC's Proposed Certificates of Compliance Rules
- DOJ and FTC State that Antitrust is Not a Roadblock to Cybersecurity Information Sharing

The DOJ/FTC policy statement is another way the Obama Administration is assisting the critical infrastructure industry to protect itself, and the nation, against cybersecurity attacks. President Obama's February 2013 Executive Order 13636, Improving Critical Infrastructure Cybersecurity, recognized cyber threats as "one of the most serious national security challenges we must confront" and highlighted the critical need for private entities to share information about cybersecurity in order to secure the nation's IT infrastructure. The Order instructed the National Institute of Standards and Technology (NIST) to develop a set of voluntary standards and processes that private industry, particularly critical infrastructure, could use to address these cyber risks. More information about the recently issued NIST Framework can be found in our February 12, 2014, Client Alert.

The joint policy statement echoes a DOJ business review letter issued in 2000 to the Electric Power Research Institute (EPRI), a nonprofit organization committed to providing and disseminating science and technology-based solutions to problems facing the energy industry. EPRI had sought a statement of DOJ's antitrust enforcement intentions with respect to EPRI's proposed information exchange designed to reduce security risks in the energy industries due to the market participants and their supply chains increasing dependence on computers and interconnectivity. The Antitrust Division determined that the proposed information exchange of best practices and information related to cybersecurity vulnerabilities would not restrict competition in any of the energy-related markets because the information exchange was limited to only physical and cybersecurity issues and excluded discussions on company-specific competitively sensitive information such as price, purchasing, and future product innovations.

Anticipating the joint guidance issued on Thursday, Renata Hesse, DOJ's Deputy Assistant Attorney General for Criminal and Civil Operations, Antitrust Division, in her January 2014 speech at the Conference on Competition and IP Policy in High-Technology Industries held in Stanford, CA, stated that while the antitrust guidance to EPRI 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."

Despite this clear statement from the country's two antitrust agencies about their antitrust enforcement intentions with respect to cyber threat information exchange, companies must continue to exercise care to avoid sharing sensitive competitive information so as to limit exposure to private antitrust litigation.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com