Published on *The National Law Review* https://natlawreview.com

DOJ (Department of Justice) and FTC (Federal Trade Commission) Opine on Information Sharing: When Cybersecurity Is Threatened, Antitrust Laws Are Not – If Properly Done

Article By:

Antitrust Litigation & Competition Regulation

In an April 10, 2014 joint policy statement (Policy Statement),[1] the Antitrust Division of the Department of Justice and the Federal Trade Commission expressly reassured entities seeking to share information concerning cybersecurity threats that it could be accomplished without raising antitrust concerns. While Assistant Attorney General Bill Baer said in his prepared remarks[2] that the legitimacy of "properly designed" cyber threat information sharing is an "antitrust no-brainer," the Policy Statement is noteworthy for several reasons.

First, the issuance of the joint Policy Statement by the two federal antitrust enforcement agencies underscores not only the generally heightened public concern about cybersecurity in view of recent attacks on retailer databases, among others, but also the visible focus on information security and privacy issues by federal antitrust leadership in the current Administration. For example, FTC Commissioner Julie Brill (a Democrat appointed in 2010) has been outspoken on issues of robust data security measures as well as data collection practices, even appearing at length on "60 Minutes" earlier this year to raise awareness concerning the data brokering industry. Similarly, Commissioner Maureen Ohlhausen (a Republican appointed in 2012) focused on data protection and cybersecurity law during her years in private practice in Washington, D.C.

Second, information exchanges among competitors have been the subject of increasing scrutiny in recent years – not only as potential indicators of cartel behavior and other unlawful agreements in restraint of trade that may be subject to criminal prosecution by the DOJ, but also as potential concerns standing alone. Indeed, just last year, the FTC utilized its exclusive enforcement authority under Section 5 of the Federal Trade Commission Act to challenge "unfair methods of competition" in order to obtain a consent order regarding exchanges of competitively sensitive information (including future product offerings, price floors, discounting, forward-looking expansion and contraction plans, and operations and performance) between two competitors in the hair restoration business.[3] Although the FTC did not allege that any agreement resulted from these exchanges, it asserted that they facilitated coordination and created the potential for reduced expansion and price fixing, as well as lacking any procompetitive justification.

Third, the policy statement provides some guidance – even if only in the form of reiterating danger areas in types of information being exchanged and specifically reinforcing a Clinton-era business review letter – concerning information exchanges generally.

The DOJ/FTC Policy Statement is not the first step undertaken by the Administration to facilitate or encourage information sharing concerning cyber threats, among private entities as well as between private entities and the government. The Administration's February 12, 2013 Executive Order 13636: "Improving Critical Infrastructure Cybersecurity,"[4] recognized cyber threats as "one of the most serious national security challenges we must confront" and required certain federal agencies to share cyber threat information (unclassified *and* classified) with targeted companies. A year later, pursuant to that Executive Order, the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, issued its "Framework for Improving Critical Infrastructure Cybersecurity," in which it stated that there should be a process for receiving cyber threat information from public-private information-sharing fora.[5]

Because well-counseled competing businesses could nevertheless be expected to harbor antitrust concerns about information sharing generally, the Policy Statement can be seen as the logical and necessary next step in the Administration's efforts. In the statement, the agencies referred to guidance in a 2000 business review letter the DOJ provided to the Electric Power Research Institute (EPRI), stating that it had no intention at that time of bringing an action against EPRI regarding a proposed information exchange designed to reduce cybersecurity risks in energy industries resulting from increasing reliance on computers and interconnectivity. Then, as now, antitrust enforcement agencies would examine the business purpose, nature, and likely competitive effect of information exchanges.[6] As set forth in the *Competitor Collaboration Guidelines*, an information-sharing agreement is typically evaluated under the rule of reason to determine the overall competitive effect of the agreement in a relevant market, taking into account its business purposes.

The basic principles and analysis of the 2000 EPRI business review letter hold true for the agencies' 2014 Policy statement: (i) sharing cyber threat information can improve efficiency and network security – a valuable purpose; (ii) cyber threat information is typically highly technical in nature (threat signatures, IP addresses, and the like), as opposed to competitively sensitive information such as future prices, output, or strategic plans; and (iii) exchanging cyber threat information is unlikely to harm competition (*e.g.*, by increasing the ability or incentive of the participants in the exchange to raise price or reduce output, quality, service, or innovation).

None of this is to say that information-sharing protocols for cyber threats will be exempt from antitrust scrutiny -- only that they "should not raise antitrust concerns" if "properly designed."[7] Companies should still carefully examine both the nature and procedure for such information sharing, as well as any protocol's actual implementation, to ensure not only that it fits within the limitations and analysis of the Policy Statement but also, as the agencies expressly cautioned, that it is not "being used as a cover to fix prices, allocate markets, or otherwise limit competition."[8]

---

[1] This joint Policy Statement is available here.

[2] The remarks as prepared for delivery by Assistant Attorney General Bill Baer (April 10, 2014) are available here.

[3] *See In the Matter of Bosley, Inc., et al.*, FTC File No. 10184.

[4] Available *here*.

[5] *See* February 12, 2014 NIST press release.

[6] These principles are set forth in, among other things, the DOJ's & FTC's joint *Antitrust Guidelines for Collaborations Among Competitors* (2000) ("*Competitor Collaboration Guidelines*") is *available* here and joint *Statements of Antitrust Enforcement Policy in Healthcare* (1996) is *available* here.

[7] Policy Statement at 9.

[8] *Id.* at 9 n.21.

©2025 Greenberg Traurig, LLP. All rights reserved.

National Law Review, Volume IV, Number 167

Source URL:https://natlawreview.com/article/doj-department-justice-and-ftc-federal-trade-commission-opine-information-sharing