WHITE & CASE

Client**Alert**

Antitrust

April 2014

DOJ & FTC Release Cybersecurity Threat Information Exchange Policy

The US DOJ Antitrust Division and the FTC yesterday released a joint policy statement on the sharing of information between private parties, including competitors, to counter cybersecurity threats. The agencies acknowledge that an important way to make progress on such threats is through the legitimate sharing between private parties of cyber threat information.

The April 10, 2014 DOJ/FTC joint policy statement recognizes that the sharing of cyber threat information has the potential to improve the security, availability, integrity, and efficiency of the nation's information systems. Thus, the agencies announce that the sharing of this information by competitors is reviewed under a rule of reason antitrust analysis, which considers "the valuable purpose behind the exchange of information." While the agencies note that the sharing of competitively sensitive information such as price, cost, and output data has the potential to harm competition, the sharing of cybersecurity information is "highly unlikely to lead to a reduction in competition and, consequently, would not be likely to raise antitrust concerns."

Although the agencies' joint statement notes the applicability of the rule of reason, thetone and express language of the new policy makes it clear that the agencies "do not believe that antitrust is – or should be – a roadblock to legitimate cybersecurity information sharing." The statement describes "cyber threat information" as "very technical in nature."

Key points from the policy statement:

- **Legitimate Cyber Threat Information:** The agencies describe legitimate cyber threat information to include information about cybersecurity threats, such as incident or threat reports, indicators, threat signatures, and alerts. Such information is typically technical in nature. For example, the agencies note that signature detection information may be used to identify malware (e.g., a virus, worm).
- **Timing of Information Exchanges:** The policy statement notes that in prior guidance on the sharing of cyber threat information, the DOJ approved the exchange of actual real-time cyber threat and attack information. The policy statement makes clear that the legal analysis in this prior guidance remains current.
- **Format of Information Exchanges:** The policy statement makes clear that legitimate information exchanges may take place using different formats. "Sharing can take many forms – it may be *unstructured or very structured*, human-to-human or automated, or somewhere in between." (Emphasis added).

J. Mark Gidley
Partner, Washington, DC
+ 1 202 626 3609
mgidley@whitecase.com

Christopher M. Curran
Partner, Washington, DC
+ 1 202 626 3643
ccurran@whitecase.com

Peter J. Carney
Partner, Washington, DC
+ 1 202 626 3662
pcarney@whitecase.com

George Paul
Partner, Washington, DC
+ 1 202 626 3656
gpaul@whitecase.com

Jack Pace
Partner, New York
+ 1 212 819 8520
jpace@whitecase.com

John D. Donaldson
Counsel, Washington, DC
+ 1 202 637 6253
jdonaldson@whitecase.com

White & Case LLP
701 Thirteenth Street, NW
Washington, DC
20005-3807
United States
+ 1 202 626 3600

- **Process to Seek Further Guidance:** The policy statement notes that companies may seek further guidance from the agencies if they have particular concerns regarding the potential sharing of certain information.

The policy statement's analytical framework builds off of and extends earlier information exchange guidelines. The cybersecurity guidelines expand certain of the guidance articulated in the 2000 DOJ and FTC Antitrust Guidelines for Collaborations Among Competitors, the 1996 DOJ and FTC Statements of Antitrust Enforcement Policy in Healthcare, and the 1995 DOJ and FTC Antitrust Guidelines for the Licensing of Intellectual Property, as well as the DOJ's 2000 business review letter to Electric Power Research Institute, Inc. (EPRI) and earlier DOJ business reviews. These guidelines and business reviews are applied more broadly than in the narrow fields in which they initially arose. The DOJ's specific guidance to EPRI is particularly instructive, and the DOJ/FTC April 10th policy statement states that it still provides relevant guidance. In the EPRI business review letter, the DOJ stated that it had no intention to initiate an enforcement action against EPRI's proposal to exchange certain cybersecurity information, including actual real-time cyber threat and attack information. The DOJ concluded that because the information exchange was limited to physical and cybersecurity issues, and because EPRI proposed sufficient safeguards against exchanges on price, purchasing and product innovations, the proposal did not raise antitrust concerns.

The DOJ/FTC cybersecurity policy statement is a positive step forward by the agencies to try to reduce the hesitancy that private parties may have to share legitimate cyber threat information with each other, especially with their competitors. The agencies' joint guidance will assist companies by describing the sharing as clearly serving a legitimate business purpose and highly unlikely to raise antitrust concerns. The sharing of information beyond that described above may also be permissible "if appropriate safeguards governing information sharing are implemented to prevent or minimize" the disclosure of competitively sensitive information.

By its nature, the agencies' joint statement gives businesses, the courts, and other decision-makers guidance and comfort as to the sorts of information exchanges which should not raise antitrust concerns at all. And the guidance is also useful in updating and extending aspects of prior agency guidance.

To read the full DOJ/FTC release click here.

This Client Alert is provided for your convenience and does not constitute legal advice. It is prepared for the general information of our clients and other interested persons. This Client Alert should not be acted upon in any specific situation without appropriate legal advice and it may include links to websites other than the White & Case website.

White & Case has no responsibility for any websites other than its own and does not endorse the information, content, presentation or accuracy, or make any warranty, express or implied, regarding any other website.

This Client Alert is protected by copyright. Material appearing herein may be reproduced or translated with appropriate credit.

In this publication, White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case LLP, a limited liability partnership incorporated under English law and all other affiliated partnerships, companies and entities.
NY0414/IT/A/09315_4