Eyup Kun

How should revised Horizontal Guidelines in EU Competition Law play a role in enabling information-sharing practices for cybersecurity?

1. Introduction

This short opinion discusses why revised Horizontal Guidelines incorporates certain analysis regarding the information-sharing practices for cybersecurity to incentivize entities to share cyber threat information among competitors by creating more certainty.

Information sharing practices constitute an essential aspect of collective cybersecurity. Those defending networks and information systems need to share "information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools''. This sharing helps

- preventing, detecting, responding to or mitigating incidents;

- enhance the level of cybersecurity, in particular through raising awareness about cyber threats, limiting or impeding such threats' ability to spread;

- supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection techniques, mitigation strategies, or response and recovery stages.

EU Commission proposed to update Network and Information Security Directive (henceforth "NISD2") in December 2020. One of the European Commission's aims in NISD2 is to "facilitate secure, robust and appropriate information-sharing".

However, there is a general uncertainty of competition law concerns regarding the information sharing between different entities, including competitors because this type of information sharing is generally based on information sharing arrangements and can be concluded among competitors.

The second section will discuss the current version of the NISD2 and its reference to the EU competition rules and why it does not provide any further clarity. The third section shed light on how the US provides more clarity regarding antitrust concerns concerning information sharing in cybersecurity. The fourth section investigates how the revised Guidelines can provide more certainty.

2. NISD 2 and its Reference to EU Competition Law

Article 26 of the proposed NISD2 requires Member States to "ensure that essential and important entities may exchange relevant cybersecurity information among themselves" while respecting the General Data Protection Regulation (GDPR). Recital 67 states that with cyber threats growing increasingly sophisticated and complex, effective detection and prevention strategies rely heavily on regular threat and vulnerability intelligence sharing between institutions. Information sharing adds to enhanced awareness of cyber dangers, which improves organizations' ability to avoid threats from materializing into actual incidents and to contain the effects of incidents more effectively. Without guidelines from the Union, various issues appear to have hampered intelligence sharing, most notably doubt about compliance with ***competition*** and liability rules.

Recital 68 states that entities should be encouraged to pool their expertise and experience at the strategic, tactical, and operational levels to strengthen their capacity to analyse, monitor, defend against, and respond to cyber threats effectively. Thus, it is vital to facilitate the establishment of platforms for voluntary information sharing at the Union level. For this purpose, Member States should

actively promote and encourage participation in such information-sharing arrangements by relevant entities that are not covered by this Directive. These processes shall be carried ***out in full conformity with the Union's competition rules*** and with the Union's data protection standards.

While the NISD2 provides a framework that enables voluntary information sharing among competitors, it provides only reference to the EU competition law without any specific guidance.

3. The US Example: No Violation of Antitrust Law in Cybersecurity Information Sharing Act

On December 18, 2015, President Barack Obama signed the Cybersecurity Information Sharing Act of 2015 ("CISA"). The law is composed of two major components. To begin, it empowers businesses to monitor and defend their information systems against cyber threats. Second, CISA provides some protections to encourage businesses to exchange information freely with the federal government, state and local governments, and other businesses and private entities – specifically, information regarding "cyber threat indicators" and "defensive measures." These safeguards include liability protections. The protections intended to entice businesses to share information were intended to address concerns that sharing information with the government or other parties could expose them to litigation for violating privacy and ***antitrust laws,*** as well as to disclosure under the Freedom of Information Act and waiver of privilege.

The Guidance states that CISA 2015 requires that the action authorised by CISA 2015 ***does not violate federal or state antitrust laws,*** including the Clayton Act (15 U.S.C. 12), the Federal Trade Commission Act (15 U.S.C. 45), and state antitrust laws that are consistent with or modelled after those laws. The antitrust provisions of CISA 2015 apply to information exchanged or assistance provided for:

(1) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information stored on, processed by, or transiting an information system; or

(2) communicating or disclosing a cyber threat indicator to assist in preventing, investigating, or

(3) mitigating the effect of a cybersecurity threat to an information system.

The antitrust provisions in CISA 2015 supplement a policy statement issued in May 2014 by the Department of Justice's Antitrust Division and the Federal Trade Commission, which stated that "a properly planned sharing of cybersecurity threat information is unlikely to pose antitrust problems." Through this Statement, the Department of Justice's Antitrust Division and the Federal Trade Commission explain their analytical framework for information sharing and make it clear that they do not believe that antitrust is – or should be – a roadblock to legitimate cybersecurity information sharing since cyber threat information typically is very technical in nature and very different from the sharing of competitively sensitive information such as current or future prices and output or business plans.

4. The Role of Revised Horizontal Guidelines

As it is stipulated under Section 2, the NISD2 provides a framework for information sharing practices to ensure cybersecurity and incentivizes information sharing. Regarding competition law concerns, it refers to competition rules without providing further guidance in the proposed NISD2. The revised Horizontal Guidelines contain an analytical framework for information sharing practices among competitors for compliance with Article 101 of the TFEU. However, there is no specific mention of cybersecurity information sharing practices to facilitate these information-sharing activities. The revised Horizontal Guidelines can provide further clarity on the cybersecurity information sharing

practices in cybersecurity to incentivize these types of information sharing among competitors. In that way, it would pave the way for the future implementation of the proposed NISD2 Directive.