Cybersecurity and Antitrust – Learning from Mistakes

17 November 2020

Margrethe Vestager, EU commissioner for competition policy, recently issued a stern public warning to car manufacturers. The European Commission is currently investigating the companies for their role in Germany's infamous car emissions scandal. Businesses that intend to cooperate in the area of cybersecurity would do well to reflect on the commissioner's warning as well. Cars and IT? At first glance, few parallels come to mind between the traditional automotive sector and the relatively new field of cybersecurity. Yet both areas face disruptive technological challenges that companies can only overcome together. The cautionary tale of the German carmakers offers vital antitrust lessons for technical cooperation far beyond the confines of the automotive industry.

Cybersecurity: Better Together?

Cross-industry digitalisation, the emergence of the Internet of Things (IoT) and a multitude of new digital technologies offer significant opportunities for nearly all industries. However, these developments create new challenges in the field of cybersecurity. Cyberattacks are estimated to cost the global economy USD 6 tn in 2021. While government measures and regulatory standards – such as the EU-wide cybersecurity certification framework established by the EU Cybersecurity Act – will play a crucial role, businesses will bear most of the future costs of cybersecurity. The sheer number of billions of connected digital devices in the EU alone further increases the need for cooperation between manufacturers to ensure security and interoperability. It is likely that companies will seek to tackle the issue together to share the immense costs of cybersecurity.

It therefore comes as no surprise that stakeholders are increasingly recognising the benefits of cooperation: In February 2018, partners from industry, politics and science launched the initiative "Charter of Trust". Their aim is to establish minimum standards along the production chain and to promote joint research and development in the field of cybersecurity. Multinational technology companies, such as Huawei, are publically calling for common cybersecurity standards in the telecommunications sector. And the Cyber Security Summit of the Munich Security Conference of 2019 also focused on multi-stakeholder cooperation against cyberattacks and disinformation.

Increased cooperation in the area of cybersecurity can help compensate for information asymmetries vis-à-vis attackers and identify frequent attack patterns. Data theft, phishing, blackmail, industrial espionage, targeted sabotage and other dynamic risks require joint solutions. However, can cooperation itself become a risk?

The Automotive Industry – a Cautionary Tale

It is worth briefly considering the automotive industry, which, for some time now, has also been facing challenges that require joint solutions. Most notably, rising environmental protection standards require novel concepts that can often only be realised on an industry-wide level. Competitors have quickly realised that there is a need for cooperation. However, their example also illustrates how crucial it is that companies are aware of the limits imposed by competition law even before they enter into a cooperation.

Recent antitrust cases show that supposedly merely technical cooperation between competitors carries an increased risk of facilitating anti-competitive agreements: Several high profile investigations against automotive suppliers have already lead to fines amounting to several hundred million Euros. In an ongoing case, the European Commission is investigating well-known German car manufacturers, which the Commission accuses of having breached EU competition rules for years. In a working group dubbed the "circle of five", the manufacturers primarily discussed technical issues, such as common quality requirements and test procedures, the exchange of technical expertise and the bundling of their developing efforts in the field of vehicle safety. However, as part of their dialogue on environmental protection, the manufacturers also discussed how to implement technical solutions for emission controls. It appears that this may have been a costly mistake.

The European Commission alleges that the manufacturers violated EU antitrust law by colluding to restrict competition on innovation for emission cleaning systems of passenger cars. The Commission is assessing whether the alleged cartel members denied consumers the opportunity to buy less polluting vehicles, despite better technology being available to the manufacturers.

What lessons can competitors seeking to cooperate in the area of cybersecurity draw from the case? To avoid any suspicion of a cartel agreement in the first place, they should heed the explicit warning issued by commissioner Vestager: *"Companies can cooperate in many ways to improve the quality of their products. However, EU competition rules do not allow them to collude on exactly the opposite: not to improve their products, not to compete on quality."*

Joint Cybersecurity R&D: What to Keep in Mind

Joint research and development can increase efficiency and is therefore privileged under antitrust law. Through cooperation in the field of cybersecurity, too, market participants could benefit from synergy effects, combine innovative strength and quickly advance the market maturity of new solutions.

However, cooperation that extends beyond the research and development of new safety products, standards or strategies can be critical from a competition law perspective. There is often only a fine line between pro-competitive research and development agreements that lead to innovative products and those that facilitate illegal coordination or foreclosure of key technologies.

In practice, cooperation regularly encompasses agreements on joint marketing of research results, licensing or production. Such cooperation, especially between competitors, requires a thorough case-by-case assessment under antitrust laws: What are the market shares of the companies involved? To whom and under what conditions will the acquired know-how be made available? Are companies still permitted to carry out their own parallel R&D activities? Will the agreement lead to a restriction of (potential) competition? Is there a risk of market foreclosure? Lastly, does the focus lie on efficiency-enhancing effects that justify joint research and marketing?

Companies involved in cybersecurity initiatives with other industry players should therefore assess any R&D projects from a competition law perspective before their implementation. They should also implement robust compliance systems. Only by preparing ahead of time can businesses mitigate risks and ensure that permitted forms of cooperation do not spill over into unlawful coordinated behaviour during the course of the cooperation.

New Technologies and Standards: How to Avoid Pitfalls

Ideally, cooperation that complies with competition law leads to the development of new key technologies and the establishment of innovative technical standards for cybersecurity. However, as the example of the car manufacturers shows, there are major risks involved. If standards or key technologies are established for an entire industry or along the entire value chain, caution should be exercised even in cases of supposedly obvious innovations.

Harmonised cybersecurity standards can reduce the incentive for innovation and further development. Once a key technology is established on a market-wide basis, it can effectively act as a barrier to entry for developers of competing technologies. The risk of market foreclosure increases if a cybersecurity initiative involves technical specifications for which patents or other intellectual property rights exist. Without

access to relevant technologies, competitors could be at risk of being excluded from competition altogether.

In practice, infringements of competition law can best be avoided through transparency. This means that all companies concerned should have the opportunity to participate in the development of an industry standard and to propose alternative solutions. When competitors are unable to switch to alternative technologies, antitrust laws may require, under certain conditions, that all market participants are granted equal access to that standard. The patent holder may then have to undertake to grant the technology in question on fair, reasonable and non-discriminatory terms (so-called FRAND commitments). Thereby, third parties can obtain access to essential technologies even against more powerful competitors. Whether such a claim exists requires a thorough assessment on a case-by-case basis. If a claim concerns accumulated data – not unlikely in the area of cybersecurity –, companies must balance antitrust and data protection requirements.

Conclusion

As the automotive industry's example shows, it is crucial for companies to carefully assess potent

ial implications of technical cooperations right at the start. In the fight against cyber threats they should be mindful of competition law requirements and thoroughly review both their security infrastructure and existing antitrust compliance measures. Businesses should also be aware of the pending 10th amendment to the German Act against Restraints of Competition (GWB). According to the latest proposal of the Federal Ministry of Economic Affairs and Energy, the revised GWB will provide for antitrust access rights to data and simplified conditions for the adoption of interim measures in the digital sector by the Federal Cartel Office.

BLOMSTEIN will closely monitor and inform about further developments. If you have any questions about the potential effects of cybersecurity on your company or your industry, Anna Huttenlauch, Max Klasse and Philipp Trube will be happy to assist you at any time.