Kluwer Competition Law Blog

The Case of Microsoft: Why Software Monocultures Also Play a Role Beyond Antitrust Considerations

Dennis-Kenji Kipker (University of Bremen) · Wednesday, September 13th, 2023

After the rumor mill had been bubbling for weeks in advance, it became official at the end of July 2023: the European Commission announced on its website the initiation of official antitrust proceedings against the US software giant Microsoft due to possible anti-competitive behaviour in relation to Microsoft Teams.

The legal background of the EU Commission is the fear that Microsoft, by bundling Teams and products from the Microsoft Office segment, could abuse and defend its market position in productivity software and, thereby, unlawfully restrict competition in the European Economic Area as far as communication and collaboration products are concerned. These legal concerns were based in particular on the distribution advantage Microsoft gains by not allowing its customers to choose whether to use Microsoft Teams or alternative products for virtual communication. The EU Commission's investigation under competition law is based on Article 102 TFEU, which prohibits the abuse of a dominant market position. Such a dominant position could in particular affect trade between the Member States and, thus, lead to distortions in the internal market. On the one hand, the legal outcome of these European antitrust proceedings will certainly be eagerly awaited – but on the other hand, Microsoft's actions also have implications for cybersecurity compliance beyond the antitrust perspective, which will be described in more detail below.

How cybersecurity regulation and competition law work together

In the area of legal regulation of cyber security, the requirements of European law have grown considerably in recent years – both in terms of the number of companies affected, but also with regard to the technical and organizational measures that must be implemented by both public institutions and private companies.

First and foremost, the Network and Information Security Directive II from 2022 should be mentioned here, but also the draft for an EU Cyber Resilience Act, which is expected to pass the European Parliament in 2024. In general, these legal acts state that cybersecurity must be implemented according to the current "*state of the art*" of technology – and it is precisely at this point that problems arise with regard to the cybersecurity compliance of Microsoft products and the monopolization of IT infrastructure triggered by the group's software bundling practices.

Why software monocultures are dangerous for cybersecurity compliance

Although Microsoft's products are used extensively by government agencies and institutions as well as private companies worldwide, they are by no means free of cybersecurity vulnerabilities. This is impressively demonstrated by the recent significant cybersecurity incident in the U.S., where, according to Microsoft, Chinese hackers managed to gain access to the email servers of various U.S. government agencies. This exploitation of a previously unknown vulnerability allowed them to tap confidential content unnoticed for weeks.

The attackers used a so-called MSA key from Microsoft to create tokens for accessing Microsoft Outlook Web Access and Outlook.com. Due to a vulnerability in the verification systems for these tokens, the attackers were also able to use them to gain access to e-mail services for enterprise customers, for whom log-in is actually controlled via other, separate systems. This vulnerability and the way it was dealt with shows more than clearly why a rethink is urgently needed in cybersecurity compliance – and why, in Microsoft's case, cybersecurity law and competition law issues are definitely closely related, because effective cybersecurity not only concerns general corporate due diligence obligations under company law, but also affects the software used in a corporation or a public authority. In addition, cybersecurity risks for Microsoft products are by no means new: over the past five years, for example, more than 170 highly critical vulnerabilities have been identified in Microsoft Exchange alone, most of which led to serious problems.

As a result, the company was responsible for one-third of all exploited vulnerabilities in the U.S. Cybersecurity and Infrastructure Agency's (CISA) Known Exploited Vulnerabilities Index in 2022 and for nine of the 15 most frequently exploited vulnerabilities in 2021. What's more, the report, published jointly by U.S. agencies CISA, NSA and FBI on Oct. 6, 2022, also clearly states that 20 percent of the largest vulnerabilities since 2020 were exploited by the People's Republic of China, and much of that involved Microsoft systems.

Microsoft has a long tradition of antitrust relevant campaigns

However, this is only one side of the coin, because at this point at the latest, the software monocultures come into play, which have been built up for decades by Microsoft's questionable approach to competition law.

An example from the deep past of the Internet in the early 2000s: Microsoft's linking of its Windows operating system with Internet Explorer. We are all aware of the fact that there is no such thing as one hundred percent cyber security. Accordingly, the compliance requirements under European law on cyber security do not presuppose this. Rather, in addition to the implementation of the current state of the art of technology in cybersecurity, they only require that a risk assessment of the protected interests is to be taken in order to arrive at an "*appropriate*" result for cybersecurity. This means, for example, that particularly important and sensitive data in a company or public authority must be subject to a higher level of cyber security than normal data. This ongoing IT risk, however, can also be exploited by attackers, who prefer to attack monopolistic software structures that have been and are being built up through the anti-competitive exploitation of market monopolies. The situation here can be compared to a forest: such forests, which are pure monocultures, are significantly more susceptible to pest attack than robust mixed forests.

Thus, monopoly-like market positions in certain software segments are particularly conducive to compromising software security, because it is always technically easier for an attacker to compromise the defenses of already known and recurrently identical systems than to have to constantly respond to a highly volatile software market characterized by numerous and diverse companies. And it was precisely this idiosyncrasy that the Chinese cyber attackers took advantage of when they planned their successful cyber-attack on the U.S. government IT services. It should be noted that the case of the U.S. government is only one case in which insecure Microsoft products resulted in a data leak. However, it is conceivable that there are many other similar cases in which the compromise of Microsoft-based IT systems has not yet been noticed.

However, this danger for cybersecurity, which arises from the monopolization of the software market, should have been counteracted already years ago. This also applies to the case of the current European antitrust proceedings, because competitor Slack Technologies already filed its complaint against Microsoft in July 2020 – now, more than three years later, the facts are only being taken up by the EU Commission. And it is definitely a successful tactic with which Microsoft acts to exclude competition: first, the company works with assurances, and the corresponding proceedings are postponed until the competition has effectively been eliminated from the market. In the end, no legal antitrust proceedings will help.

Walled gardens are dangerous for innovation and digitization

Instead of, thus, counteracting such monopolization and its risks for cybersecurity, it is increasingly and specifically being exacerbated, especially in the software market. And ultimately, cybersecurity is also closely linked to the issues of innovation and digitization, which also have considerable political relevance in the European Union. For example, monopoly-like entrepreneurial positions harm small startups and scale ups by deliberately preventing any form of competition – be it through the bundling of software packages, but also through a corresponding pricing policy. Here, too, Microsoft has been able to prevail over competitors such as Opera or Firefox with its Internet Explorer and now Edge web browser. Thus, the debate about the integration of Microsoft Teams into Microsoft Office, which has been going on publicly since July, makes it very clear that the antitrust investigation currently being conducted by the European Commission is not taking place for no reason, but that the U.S. corporation is quite the opposite, deliberately exploiting its dominant market position to outmaneuver smaller competitors from the outset.

Unbundling alone cannot be a sustainable solution

The antitrust problems described above will not be solved by the fact that Microsoft announced shortly after the opening of the European antitrust proceedings that it would abolish the product bundling of Microsoft Teams with the group's Office products. Quite the opposite: such an approach makes it clear that the group is not actually interested in giving users the right to choose or in promoting free competition for the development of the best available technology. In conclusion, this approach certainly cannot be described as "proactive change", as Microsoft describes the concession in a press release. Nor does such an approach change Microsoft's general corporate policy of first creating facts on the market by violating competition rules and then giving

in in a way that attracts publicity and media attention in a positive way. The damage to technology development and effective cybersecurity has already been done, and not only in the field of web-based communication technology.

We need more than just a legal perspective

This somewhat different perspective on the European antitrust proceedings against Microsoft illustrates that competition proceedings, particularly in the technology sector, can certainly have even more far-reaching effects than the mere abstract antitrust legal dimension. Moreover, it is questionable whether the legal outcome of these proceedings can be at all capable of eliminating the considerable grievances on the EU software market, the foundations of which were laid as early as the 1990s. After all, the problem of software monocultures is by no means new, but has been established for years and continues to be so. For example, government customers in both the U.S. and Europe are bound by contractual software licensing agreements that – perhaps out of their own convenience – are no longer questioned. However, a simple "*business as usual*" can no longer exist in the wake of the massive increase in cyber threats and the drastically changed global political situation, as well as with regard to the uprising situation we face in cybersecurity legal compliance issues. In addition, the lack of choice of providers and the lack of competition, especially in the public sector, has not only driven up the prices for digital services, but has rather become the basis for an ideal attack surface.

But how should we now deal with this considerable competition law dilemma that has grown over decades? The solution to the question is actually obvious: monocultures in the software industry can only be broken up by more natural competition and innovation. And at this point, the legislator must be called into action by regulating the global software industry – and Microsoft is just one precedent here – much more strongly than before by prohibiting anti-market licensing and product bundling practices. It should no longer be the case that, simply because you are using a provider for x, you will be penalized for using a different provider to do y. Regulators must step in to ensure that there is room for smaller companies across Europe to provide access to services without the risk of being pushed out by a current provider and this should start at the very top through government procurement processes.

This requires clear regulations for the national competition authorities – which is why the outcome of the European Commission's current antitrust proceedings against Microsoft is all the more important, as it will be a decisive factor not only for competition law but also for European cybersecurity compliance in the future. The handling of these proceedings will undoubtedly set the precedent for future competition issues and it is imperative that the relevant authority is taking them seriously. There needs to be a much more efficient and effective process for dealing with competition issues early on rather than waiting until it is too late and we should welcome any regulation around fair competition practices across all software licensing and bundling in the EU.

---

please subscribe here.

Kluwer Competition Law

The **2022 Future Ready Lawyer survey** showed that 79% of lawyers are coping with increased volume & complexity of information. Kluwer Competition Law enables you to make more informed decisions, more quickly from every preferred location. Are you, as a competition lawyer, ready for the future?

Learn how **Kluwer Competition Law** can support you.

This entry was posted on Wednesday, September 13th, 2023 at 9:00 am and is filed under Source: OECD">Abuse of dominance, Cybersecurity, European Commission, European Union, Innovation, Tying and Bundling
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.