

Merger: main developments between 1 January and 30 April 2011

by John Gatti

Introduction

The Commission received 93 notifications between 1 January and 30 April 2010. This is a slight increase over the previous four months and over the corresponding period of 2009. The Commission adopted a total of 84 first phase decisions, of which 82 were unconditional clearances. Decisions adopted under the simplified procedure accounted for 60 of the first phase total, or 70 %. Two first phase transactions were cleared conditionally. One case was withdrawn in Phase I. There was one prohibition decision adopted under Article 8 after an in-depth second phase investigation. Five decisions were taken under Article 4(4) to refer a case with a Union dimension back to a Member State. Of these, four were complete referrals and one was for a partial referral. Member States accepted eight requests from parties for cases to be referred to the Commission and refused none under Article 4(5). Finally, the Commission made one complete referral to a Member State, following a request made under Article 9.

Summaries of decisions taken in the period

Summaries of decisions taken under Article 6(2)

GDF Suez/International Power

The European Commission cleared on 26 January the proposed acquisition of International Power plc of the United Kingdom by GDF Suez S.A. of France, both active in the energy sector. The regulatory clearance is conditional on the divestment of International Power's shareholding in T-Power, the owner of a Belgian power plant due to start production in 2011, and the transfer to third parties of the operation and maintenance agreement of the T-Power plant.

GDF Suez has activities along the entire energy chain all around the world. International Power is an international operator of power generation facilities with activities in North America, Europe, the Middle East, Australia and Asia.

The Commission's investigation showed the absence of competition concerns on most of the relevant markets due to the minor horizontal overlaps

between the parties' activities. The only exception was the two firms' operations on the Belgian market for the generation and wholesale of electricity. There, the Commission found that the proposed transaction, as initially notified, would have raised concerns, since it could have enabled GDF Suez to use sensitive information regarding the T-Power plant and its discretion over the operation of the plant to raise electricity prices in the Belgian wholesale market and to put its competitor, RWE Essent, at a competitive disadvantage on this market. Consequently, the proposed transaction would have further strengthened the position of the market leader GDF Suez, reducing the gains of market liberalisation. To resolve these competition concerns, the parties proposed to divest International Power's shareholding of T-Power and to transfer to third parties the operation and maintenance agreement of the T-Power plant.

In view of the remedies proposed, the Commission concluded that the proposed transaction, as modified, would not significantly reduce competition in all or part of the European Economic Area (EEA). This decision is conditional on full compliance with the commitments.

The Commission cooperated closely with the Belgian Competition Authority throughout the investigation. On 20 December 2010, the Belgian Competition Authority requested the Commission to refer to it the examination of the proposed transaction pursuant to Article 9 (2)(a) of the Merger Regulation. However, in the light of the commitments offered by the parties, the Belgian Competition Authority withdrew its referral request on 19 January 2011.

Intel/McAfee

Also on 26 January 2011, the European Commission approved the proposed acquisition of McAfee, a vendor of information technology security, by Intel, both of the US. The approval is conditional on a set of commitments ensuring fair competition between the parties and their competitors in the field of computer security, a growing concern due to the exponential rise in malware such as viruses. The Commission was concerned that rival IT security products could be excluded from the marketplace, given Intel's strong presence in the world markets for computer chips and chipsets. In particular, the Commission was worried about the high likelihood

that the merged entity would embed its own security solutions into its chips and chipsets. To alleviate those concerns, Intel committed itself to ensuring the interoperability of the merged entity's products with those of competitors.

Intel is the leading manufacturer of central processing units ('CPUs'), the core chip of a computer, and chipsets, which are used in industries such as computing and communications, and are among the most important components of computers. Intel also develops platforms of digital computing technologies, which combine various types of hardware and software.

McAfee is a security technology company active in the design and development of security products and services focused on ensuring that internet-connected devices are protected from malicious content.

Intel and McAfee are active in neighbouring and complementary product markets. The merger's effects, therefore, were measured not in terms of overlaps of products and services, but rather in terms of conglomerate effects. In addition, security solutions vendors need, *inter alia*, access to specific information regarding CPUs to be able to develop new solutions.

The Commission's investigation identified serious competition concerns regarding the possible bundling of CPUs and chipsets, on the one hand, with McAfee's security solutions, on the other.

In particular, the Commission was concerned that, as a result of the proposed transaction as initially notified, other companies' security solutions might have suffered from a lack of interoperability with Intel CPUs and chipsets or from a technical tying between the latter and McAfee's security solutions. The Commission was also concerned about possible effects on Intel's competitors if McAfee solutions were no longer compatible with non-Intel CPUs and chipsets.

In order to address the Commission's concerns, Intel committed itself, among other things, to ensuring that vendors of rival security solutions would have access to all necessary information to use functionalities of Intel's CPUs and chipsets in the same way as functionalities used by McAfee. Intel also made a commitment not to actively impede competitors' security solutions from running on Intel CPUs or chipsets. Finally, Intel will avoid hampering the operation of McAfee's security solutions when running on personal computers containing CPUs or chipsets sold by Intel's competitors.

The Commission concluded that the commitments were suitable to remove the competition concerns identified while preserving the efficiencies of the

merger, because they are designed to maintain interoperability between the merged entity's products and those of their competitors, thereby ensuring competition on an equal footing between the parties and their competitors.

Summaries of cases taken under Article 8

Olympic Air/Aegean Airlines

The European Commission has prohibited on 26 January the proposed merger between Aegean Airlines and Olympic Air, as it would have resulted in a quasi-monopoly on the Greek air transport market. This would have led to higher fares for four out of six million Greek and European consumers travelling on routes to and from Athens each year. Together, the two carriers control more than 90 % of the Greek domestic air transport market and the Commission's investigation showed no realistic prospects that a new airline of a sufficient size would enter the routes and restrain the merged entity's pricing. The companies offered to cede take-off and landing slots at Greek airports, but Greek airports do not suffer from the congestion observed at other European airports in previous mergers or alliances.

Aegean Airlines is a publicly-listed company. Olympic Air is part of the bigger Olympic group of companies, themselves owned by Greece's Marfin Investment Group.

Aegean provides scheduled and charter air passenger transport as well as cargo transport in Greece and on international short-haul routes. It operates from Athens International Airport and serves around 45 short-haul destinations, including the Greek islands. It has been part of the Star Alliance since 2010.

Olympic consists of three legal entities: (i) Olympic Air, active since 1 October 2009, following the privatisation of the former Olympic Airlines; (ii) Olympic Handling, which offers a full range of ground handling services at 39 Greek airports, serving both Olympic Air and third party airlines; and (iii) Olympic Engineering, which is currently in start-up mode and is active in the provision of maintenance, repair and overhaul services.

Both Aegean and Olympic Air operate on routes covered by public service obligations (PSOs). Aegean has PSOs on four routes. Olympic has PSOs on 13 routes.

As with previous airline mergers, the Commission analysed the combined effects of the proposed merger on the individual routes on which both companies operate. It received views and complaints from a large number of market participants

in Greece and internationally, including consumer associations, public authorities, travel agents, airport operators, ferry operators and other airlines.

The proposed merger would have led to a quasi-monopoly between Athens and Thessaloniki, the country's second-biggest city, and between Athens and eight island airports, namely Herakleion and Chania, both in Crete, Rhodes, Santorini, Mytilini, Chios, Kos and Samos. None of these are routes covered by public service obligations.

The investigation showed that generally, ferry services are not a sufficiently close substitute for air services and would not constrain the merged entity's pricing behaviour post-merger. Their travel times are much longer and their frequencies lower. The only domestic route where ferry services were considered a close substitute for air services is Athens-Mykonos, for which the Commission concluded there were no competition problems. The market investigation did not identify any significant competition concerns in relation to the short haul international routes operated by the parties

The market investigation also showed that there was no prospect that a new player would enter the Greek market after the merger and challenge the new entity on a scale sufficient to constrain the combined entity's behaviour on domestic flights to and from Athens.

The companies offered to release slots at Athens and other Greek airports, as well as other remedies, such as access to their frequent flyer programmes and interlining agreements. However, the nature and the scope of these remedies were insufficient to ensure that customers would not be harmed by the transaction. This is notably because the main problem in this case — unlike previous airline cases — was not the availability of slots, which are available at Athens airport and at most Greek airports. The market test also showed that the remedies were unlikely to entice a credible new player to create a base at Athens airport and exert a credible competitive constraint on the affected routes.

The Commission, therefore, concluded that the concentration *'would significantly impede effective competition in the internal market or a substantial part of it'* (Art 2.3 of the Merger Regulation) and prohibited the transaction. The elimination of competition

which would have been associated with the merger would have been harmful for Greek customers.

Summaries of cases taken under Article 9

Thomas Cook/Travel Business of Midlands Cooperative Society

On 7 January 2011, following a request by the United Kingdom's Office of Fair Trading (OFT), the European Commission referred the assessment of the proposed acquisition of the travel businesses of Cooperative Group (CGL) and of Midlands Cooperative Society (Midlands) by Thomas Cook to the UK authorities. CGL and Midlands are active in the UK only. After a preliminary investigation, the Commission found that the proposed concentration threatens to give rise to competition concerns in the market for holiday distribution and in particular the distribution of package holidays in the UK.

Thomas Cook is active across Europe as a leisure tour operator and a distributor of travel services via its travel agency network. It is one of the two major integrated leisure travel companies in the UK, the other being TUI Travel.

The travel businesses of CGL and Midlands are focused on the retail distribution of holiday products in the UK. While CGL has high street travel agencies across the country, the agencies of Midlands are mainly located in the Midlands regions.

The OFT requested the Commission to refer the notified concentration for review to the UK authorities under Article 9 of the EU Merger Regulation. It was concerned that the transaction threatened to affect competition significantly in the distribution of holidays via retail travel agency outlets in the UK and a number of affected UK regions.

The Commission's preliminary investigation confirmed that the proposed transaction raised competition concerns in a distinct market which was at most UK-wide. Moreover, the Commission considers that the UK competition authorities are well placed to investigate the effect of the transaction on the national market or parts of this market. As CGL and Midlands are not active in other Member States, any possible competition problems are confined to the UK. The Commission therefore decided to refer the case in its entirety to the UK competition authorities for review.

Intel/McAfee (1)

by Jocelyn Guitton, Adrian Lübbert, Isabelle Neale-Besson and Jérôme Vidal (2) (Unit C5)

1. Introduction

On 26 January 2011 the European Commission approved the proposed acquisition of McAfee by Intel, both of the US. The approval is conditional upon a set of commitments ensuring fair competition in the sector of computer security. Computer security is a growing concern due to the exponential rise in the number of malware (3) present on the internet, as well as their possible consequences, in particular for large enterprises and governments.

The case raised technically complex issues and triggered negative reactions from third parties in the IT sector, including competitors and customers of both Intel and McAfee. However, following an extensive investigation into the security software market, a conditional clearance decision was reached at the end of the first phase review.

2. A conglomerate case

Intel is the leading producer of central processing units (“CPU”) and chipsets. The CPU is the device within an electronic device (e.g. a computer) that interprets and executes instructions. It is the computer’s ‘brain’. CPU performance is a key component in the overall performance of a computer. A CPU is also the component which represents the most significant proportion of a computer’s cost. A chipset refers to a designated group of integrated circuits. Its main task is to connect the CPU to other components, such as the main memory, graphics controllers and peripheral devices. Chipsets are generally designed to work with a specific family or generation of CPUs.

McAfee is a security technology company active in the design and development of IT security products and services. IT security solutions pursue two main objectives: (1) detection of and defence against incoming threats and (2) control and certification of authorised users and software. McAfee supplies security solutions for servers, desktops and laptop

computers, handheld voice and data phones, and other devices that are connected to corporate systems and networks and home PCs.

The products of Intel and McAfee are closely related from both a technical and a commercial point of view. On the technology side, for reasons of security and speed, security software interacts directly with the hardware level (CPU, chipset), perhaps to an even greater extent than other software. Security software vendors (“SSVs”) therefore need access to up-to-date, accurate and complete interface information on new CPUs and chipsets in order to be able to develop new security software. Good interface information is also required in order to optimise the software with regard to performance and power consumption, since the running of security processes may significantly increase the workload on the CPU and affect the available performance of the computer. Moreover, certain features of IT security may be more effectively enabled in hardware than in software. For instance, a user’s digital signature, required for encryption and authentication, can be stored and generated more securely in hardware.

On the commercial side, every endpoint working on a Windows/x86 (4) platform needs in principle some form of security software in order to be protected against incoming threats. Moreover, the same intermediaries, such as Original Equipment Manufacturers (“OEM”) or Value Added Resellers in the enterprise market, may be involved in the decisions regarding which CPUs to use and which security solution to install.

Given the technological and commercial context, the merger’s effects would be conglomerate, rather than horizontal overlaps of products and services.

In most circumstances, conglomerate mergers do not give rise to competition problems. However, in some cases - particularly where, as in the present case, the merged entity enjoys strong market power in one of the markets concerned - a conglomerate

(1) Commission Decision n°COMP/M.5984 – *Intel/McAfee*, 26 January 2011.

(2) The content of this article does not necessarily reflect the official position of the European Commission. Responsibility for the information and views expressed lies entirely with the authors.

(3) Malware, short for malicious software, is a software designed to secretly access a computer system without the owner’s informed consent.

(4) The architecture is about the way to organise the connections between transistors within the CPU. There are two main categories of computer CPUs which are based on two different conceptions of the set of instructions: Complex Instruction Set Computer (“CISC”) and Reduced Instruction Set Computer (“RISC”). Intel’s x86 instructions architecture, which is built on the basis of a CISC architecture, is the most widely used in today’s computer industry.

merger may create possibilities for bundling or tying practices or other exclusionary practices. While companies often engage in tying and bundling in order to provide their customers with better products or offerings in cost-effective ways, these practices may in certain circumstances lead to a reduction in the ability or incentive of actual or potential rivals' to compete and, consequently, this may reduce the competitive pressure on the merged entity.

3. The Commission's assessment

3.1. The markets

The Commission's phase I market investigation confirmed the existence of a separate market for x86 architecture CPUs as identified in the 2009 Commission Intel antitrust decision⁽⁵⁾. While it might be appropriate to further segment x86 CPUs according to the type of platforms (servers, desktops and notebooks) or the type of devices (PCs, handheld devices and consumer electronics), the question of further segmentation was left open since the conclusions of the assessment would remain unchanged. The Commission concluded that the relevant x86 CPU market has a worldwide geographic scope.

Chipsets could constitute a distinct product market from other hardware components, in particular CPUs, since they can be bought and sold independently. The market definition was left open since the conclusions of the assessment would remain unchanged. The Commission considered that the market for chipsets was worldwide.

The market investigation largely confirmed that the IDC segmentation of the security solution market, previously used in a decision⁽⁶⁾, was appropriate and that endpoint security could be regarded as a distinct product market. It also suggested that endpoint security may have to be further segmented according to the type of end-user, that is to say endpoint security for consumers and endpoint security for enterprises. The Commission left open the exact definition of the relevant product markets for endpoint security, as the conclusions of the assessment would be the same. The Commission concluded that the endpoint security markets had a worldwide or at least EEA-wide geographic scope.

3.2. Competitive landscape

While the x86 architecture with Intel and AMD as the main CPU producers remains pervasive for servers, desktops, laptops and netbooks, this architecture faces some competition in netbooks and strong competition in handhelds from ARM, a company that has developed a RISC architecture used in most mobile devices such as smartphones. Currently, the x86 architecture is also facing a limited degree of competition from graphic cards manufacturers (e.g. Nvidia). A GP-GPU (General Purpose Graphic Processing Unit) can to a certain extent perform the same functions as a standard CPU. In particular, a GP-GPU can handle a larger number of (parallel) computing tasks and it may reduce the demand for high-end CPUs as a result. In the competitive landscape in the overall x86 CPU market, Intel occupies a prominent position, with more than 80% of the market share of the volume shipped. AMD holds a much lower share of the market, while Via's position is very limited in terms of volume shipped.

As regards chipsets, a radical shift took place in 2008-2009 as a result of market consolidation and technological developments. Consequently, the number of market participants that are shipping significant volumes of chipsets has decreased from seven in 2005, to three in the current market situation (Intel, AMD and Nvidia). Intel's market share ranges between 70 and 80%.

The market investigation confirmed the findings of the Commission's 2009 Intel antitrust decision, in particular the Commission's analysis of barriers to expansion and entry, which are still high.⁽⁷⁾

McAfee is the number two player in the security software market behind Symantec and ahead of Trend Micro. These three companies are the only ones active in both endpoint security for consumers and endpoint security for enterprises. Only these three companies are also active to a commercially significant extent in the OEM channel, that is to say they have agreements with OEMs to pre-install security software for a free trial on the computers shipped by the OEMs. Apart from the three big vendors, there is a large number of smaller, often regional, endpoint SSVs such as Kaspersky, F-Secure, AVG, Avast, Avira, or Panda Security. In the consumer space, many of those smaller players operate on the basis of a freemium business model, that is to say they offer basic security software for

⁽⁵⁾ See paragraphs 808 and 813.

⁽⁶⁾ Commission decision n°COMP/M.3697 – Symantec / Veritas, 15 March 2005, paragraph 10. In that decision, the backup and archive software, a sub-category of the overall segment of storage software, has been identified as a relevant product market.

⁽⁷⁾ Barriers to entry and expansion identified are: (i) the significant sunk costs in research and development, (ii) the significant sunk costs in plant production and (iii) the resulting significant economies of scale which mean that the minimum efficient scale is high relative to overall market demand.

free and obtain their revenues from more sophisticated security products.

According to the Commission's market investigation, barriers to entry appear to be lower on the market for security software. In the consumer market, in particular, it appears feasible to become either a specialist niche player or an imitator, employing the freemium model. In contrast, barriers to expansion in the commercially important areas, that is to say both the enterprise and the consumer segment, seem to be significant. Economies of scale are essential in order to support the R&D and infrastructure necessary to detect new malware and update the software accordingly. The three leading SSVs - Symantec, McAfee and Trend Micro - account for a large share of the industry's R&D investments and they operate extensive global threat detection networks.

3.3. Competition problems

The Commission's concerns related to three possible types of practices, namely (i) degradation of interoperability between Intel's hardware and security solutions on the one hand and the products of competitors on the other, (ii) technical bundling/tying ("technical tying") and (iii) commercial bundling ("commercial bundling").

Interoperability can be defined as the possibility for software and hardware to interact⁽⁸⁾. Degradation can be defined as positive or negative discrimination (1) to the detriment of SSVs competing with McAfee when it comes to achieving interoperability with Intel CPUs or chipsets or (2) to the detriment of CPU or chipset producers competing with Intel when it comes to achieving interoperability with McAfee. It can take several forms, such as non-availability of certain hardware instructions or functions, delayed or incomplete disclosure of support tools and of information on hardware instruction sets and architecture.

Technical tying consists in the technical combination of products of both parties in a persistent

form, that is to say in the embedding of security solutions in Intel's CPU and chipsets platforms. In order to prevent any foreclosure on the security solutions market as a result of embedding security software into Intel's hardware, it would not necessarily be sufficient to ensure interoperability between the solutions developed by McAfee competitors and Intel's hardware. Indeed, the persistence of embedded software solutions from McAfee's software into Intel hardware could interfere with the functioning of competitors' security solutions.

Commercial bundling could take two forms. Pure bundling would mean that CPUs and security software are sold exclusively together, while mixed bundling would mean that either the CPUs or the security software would be offered at a discount when customers buy both products from Intel/McAfee.

Such business strategies could aim to leverage Intel's market power in the CPU and chipset markets into the endpoint security markets, leading to significant weakening and possible exit of McAfee's main competitors within the next two to five years. An Intel/McAfee security monoculture could ensue, reducing competition and innovation in the endpoint security markets with significant consequences for the overall security of computing devices in general.

The Commission's assessment was based on submissions made by several complainants, submissions made by third party market observers and internal documents of both Intel and McAfee obtained in the course of the investigation. The Commission found it likely that Intel would have the ability and incentives to hamper interoperability and/or to technically tie, and that the negative effects of such practices on the relevant markets would be significant. In contrast, the Commission concluded that while the investigation had revealed a certain ability on the part of Intel to commercially bundle its hardware solutions with McAfee's security software solutions, the incentives to do so seemed to be limited. Possible antitrust enforcement would also have a certain deterrent effect. Moreover, the foreseeable effects of such a strategy, taken in isolation, would probably remain limited.

4. The commitments

It should be recalled that divestitures or the removal of links with competitors are the preferred remedy to eliminate competition concerns. In the conglomerate case at stake, however, non-structural remedies appeared to be best suited to address the concerns raised. Indeed, this was a case where one of the main concerns was that control of key technology and possibly related IP rights may have led to foreclosure of competitors whose products need

⁽⁸⁾ A more general definition is given in the software copyright directive: "The function of a computer program is to communicate and work together with other components of a computer system and with users and, for this purpose, a logical and, where appropriate, physical interconnection and interaction is required to permit all elements of software and hardware to work with other software and hardware and with users in all the ways in which they are intended to function. The parts of the program which provide for such interconnection and interaction between elements of software and hardware are generally known as "interfaces". This functional interconnection and interaction is generally known as "interoperability"; such interoperability can be defined as the ability to exchange information and mutually to use the information which has been exchanged": <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:11:0016:01:EN:HTML>

to interoperate with this technology on an equal footing. In these circumstances, commitments to grant competitors access to the necessary information may eliminate the competition concerns around interoperability. In addition, as regards technical tying, SSVs need protection from practices by which Intel would leverage its dominant position into the security solutions market and hinder SSVs from offering their products.

Commercial bundling did not – in isolation – give rise to competition concerns. As Intel proposed adequate remedies to address the competition concerns around interoperability and technical tying, the Commission considered that it was not necessary for Intel to propose remedies for commercial bundling.

In order to address the Commission's competition concerns (interoperability degradation and technical tying), Intel undertook, among other things, to ensure on an ongoing basis and in a timely manner that instructions and interoperability information for new functionalities in Intel CPUs and chipsets would be documented and available for use by independent SSVs on a royalty-free basis.

Intel also committed not to actively impede competitors' security solutions from running on Intel's CPUs or chipsets. In particular, Intel committed to a mechanism to ensure that tied security could be disabled by OEMs and would not interfere with the performance of solutions provided by McAfee competitors. This means that – as opposed to a full or partial prohibition to technically tie or an obligation to effectively replace tied security – OEMs would have at least the option to replace tied security with security solutions provided by independent SSVs instead. The Commission considered that this commitment was proportionate insofar as it

did not prevent Intel/McAfee from offering new combined and innovative products on the market, but nevertheless contributed to avoiding the risk of monoculture and ensuring continued competition and innovation amongst SSVs.

These 5-year commitments will be enforced via a monitoring trustee⁽⁹⁾ and a dispute settlement mechanism, including fast-track arbitration.

Lastly, while parts of these commitments will need to be implemented in practice via agreements, the terms and conditions of which have not yet formed an integral part of the text of the commitments, Intel committed to a structured process for the Commission's approval of the standard texts for license and warranty agreements.

The Commission concluded that the commitments were suitable to remove the competition concerns identified while preserving the efficiencies of the merger. The commitments were designed to maintain interoperability between the merged entity's products and those of their rivals, thereby ensuring competition on an equal footing between the parties and their competitors.

5. The cooperation with the U.S. Federal Trade Commission ("FTC")

The US FTC also reviewed the Intel/McAfee merger and cleared it without remedies at the end of the phase I investigation on 20 December 2010. The Commission and the FTC cooperated during the respective reviews. The cooperation was close and conducted in an atmosphere of trust and mutual assistance. While the procedures and processes are different in the two jurisdictions, the Commission and the FTC essentially reached a similar outcome, namely an early approval of the transaction.

⁽⁹⁾ Mr. Olli-Pekka Kallasvuo, former CEO of Nokia, has been appointed as Monitoring Trustee.