EN

Case No COMP/M.5984 -
INTEL / MCAFEE

Only the English text is available and authentic.

REGULATION (EC) No 139/2004
MERGER PROCEDURE

Article 6(1)(b) in conjunction with Art 6(2)
Date: 26/01/2011

In electronic form on the EUR-Lex website under document number 32011M5984

Office for Publications of the European Union
L-2985 Luxembourg

EUROPEAN COMMISSION

Brussels, 26.1.2011
SG-Greffe (2011) D/1407
C(2011) 529 final

In the published version of this decision, some information has been omitted pursuant to Article 17(2) of Council Regulation (EC) No 139/2004 concerning non-disclosure of business secrets and other confidential information. The omissions are shown thus […]. Where possible the information omitted has been replaced by ranges of figures or a general description.

PUBLIC VERSION

MERGER PROCEDURE
ARTICLE 6(1)(b) DECISION IN CONJUNCTION WITH ARTICLE 6(2)

To the notifying party:

Dear Sir/Madam,

Subject: Case No COMP/M.5984 – INTEL/MCAFEE
Notification of 29.11.2010 pursuant to Article 4 of Council Regulation No 139/2004[1]

1. On 29 November 2010, the Commission received a notification of a proposed concentration pursuant to Article 4 of the Merger Regulation by which the undertaking Intel Corporation ("Intel", USA) acquires within the meaning of Article 3(1)(b) of the Merger Regulation control of the whole of the undertaking McAfee, Inc. ("McAfee", USA) by way of purchase of shares.

I. THE PARTIES

2. **Intel** is the leading central processing unit ("CPU") and chipset producer. It develops advanced integrated digital technology products, primarily integrated circuits, for industries such as computing and communications. Intel also develops platforms of digital computing technologies, which combine various types of hardware and software.

[1] OJ L 24, 29.1.2004, p. 1 ("the Merger Regulation"). With effect from 1 December 2009, the Treaty on the Functioning of the European Union ("TFEU") has introduced certain changes, such as the replacement of "Community" by "Union" and "common market" by "internal market". The terminology of the TFEU will be used throughout this decision.

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

II. THE CONCENTRATION

4. On 18 August 2010, Intel and McAfee signed a binding Agreement and Plan of Merger pursuant to which Jefferson Acquisition Corporation, a wholly owned subsidiary of Intel, will merge with and into McAfee[2]. McAfee will be the surviving entity and will become a wholly owned subsidiary of Intel. As a result of the proposed transaction, McAfee will be solely controlled by Intel. The operation therefore constitutes a concentration within the meaning of Article 3(1)(b) of the Merger Regulation.

III. EU DIMENSION

5. The undertakings concerned have a combined aggregate worldwide turnover of more than EUR 5 000 million (Intel: EUR 25 184 million; McAfee: EUR 1 382 million)[3]. Each of them has an EU-wide turnover in excess of EUR 250 million (Intel: EUR […] million; McAfee: EUR […] million), but each does not achieve more than two-thirds of its aggregate EU-wide turnover within one and the same Member State. The notified operation therefore has an EU dimension.

IV. RELEVANT MARKETS

A. Introduction

6. There is no relevant horizontal overlap or vertical relationship between Intel and McAfee. CPUs and/or chipsets and IT security solutions are however largely complementary and at least closely related products.

1. CPUs and chipsets

CPUs

7. The CPU is the device within an electronic device (mostly a computer) that interprets and executes instructions[4]. CPUs generally comprise millions of transistors that process data and control other devices in a computer system. The CPU has the ability to fetch, decode and execute instructions and to transfer information to and from other resources over the computer's main data-transfer path, the bus. The CPU is the computer's 'brain'.

8. CPU performance is a key component in the overall performance of a computer. In terms of cost, a CPU is the component which represents the most significant proportion of a

---

2 Each share of common stock of McAfee will be cancelled and converted into the right to receive cash equal to USD 48 per McAfee share.

3 Turnover calculated in accordance with Article 5(1) of the Merger Regulation and the Commission Consolidated Jurisdictional Notice (OJ C95, 16.04.2008, p1).

4 Microsoft Computer Dictionary, 5th edition, Redmond, USA, p. 132.

computer's cost. According to one study quoted by the Commission in its 2009 Intel antitrust decision[5], it ranges between 13% and 27% of the final cost of a computer (generally speaking, the higher the specification of the computer, that is, the more sophisticated the computer is, the higher the share of the cost accounted for by the CPU).

9. CPU manufacturers compete in particular on two dimensions: the architecture and the physical dimension of the transistors.

10. The architecture is about the way to organise the connections between transistors within the CPU. As regards architecture, 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.

11. The physical dimension is about the size of transistors and circuitry that can be achieved within the CPU: the smaller it is, the faster is the CPU and the less energy it consumes. As regards the physical dimension, Intel is now one of the last vertically-integrated semiconductors manufacturers, as opposed to its two competitors in x86 CPUs, AMD and Via Technologies ("Via"), who are 'fabless' manufacturers[6].

Chipset business

12. A chipset refers to a designated group of integrated circuits that is designed to perform one or more related functions. Its main task is to connect the CPU to a specified set of other components. The chipset primarily consists of a 'northbridge' and a 'southbridge', which are dedicated to connecting the CPU to the high-speed components, notably the main memory and graphics controllers, and to the lower-speed peripheral devices, respectively.

13. Chipsets are generally designed to work with a specific family or generation of CPUs: a CPU and chipset combination needs to be compatible in order to function.

2. IT security solutions

14. Information technology security has become a growing concern over the past few years, due to the exponential rise in the number of malware[7] present on the internet, as well as its possible consequences, in particular for large enterprises and governments.

15. 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[8].

---

5 Commission decision of 13.05.2009 relating to a proceeding under Article 82 of the EC Treaty and Article 54 of the EEA Agreement (COMP/C-3 /37.990 - Intel), ("the 2009 Commission Intel antitrust decision").

6 'Fabless' semiconductor companies specialize in the design and the sale of hardware devices and CPUs while outsourcing the fabrication of the devices to a specialized manufacturer.

7 Malware, short for malicious software, is a software designed to secretly access a computer system without the owner's informed consent.

8 A third essential objective is to recovery and repair after a security incident.

16. Detection of and defence against incoming threats consists in identifying incoming threats and in preventing malware from accessing information and devices by recipients or from destroying or altering that information. Traditionally this objective is often achieved on the basis of a 'black-listing' approach, where incoming elements are compared against a database of known threats. In some environments (e.g. the I-Phone platform) this objective is also achieved through a 'white-listing' approach where only software or applications listed and recognised as safe are allowed to access a given device.

17. Control and certification of authorised users and software consist in allowing access to a device, a mailbox or data only to those users, applications or software that have been previously certified as safe and which can identify themselves through a key or certificate.

3. Relationship between CPU/chipset and security solutions

Technological link

18. First, on the technology side, both for reasons of security and speed, security software interacts perhaps to a greater extent than other software directly with the hardware level. 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 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. In that connection it must be borne in mind that software vendors typically write their software at a high level of abstraction and let compilers (which translate the software language into the hardware language) adjust the code for the specificities of a CPU. In many cases, the operating system ("OS") also consolidates multiple hardware features into software functions that are easier to use and allow software to access these functions through application programming interfaces ("APIs").

19. Second, certain features of IT security may be more effectively enabled in hardware (CPU, chipset) than in software. For instance, the user digital signature, required for encryption and authentication, can be stored and generated more securely in hardware. File scanning, required for the detection of viruses, may be more efficiently performed at the level of the CPU. Hardware implemented security may also enable remote attestation which can be used to control accesses to a network. Overall, the partial embedding of security solutions in hardware may lead to more robust and/or faster security solutions.

20. The products of Intel and McAfee are therefore from a technical point of view in closely related markets.

Commercial link

21. On the commercial side, every endpoint[9] working on a Windows/x86 platform needs in principle some form of security software in order to be protected against incoming threats[10]. Moreover the same intermediaries such as Original Equipment Manufacturers

---

9 Endpoint refers to a broad array of devices, notably desktop, notebook and handheld devices.

10 Stand-alone computing platforms running Microsoft Windows are currently the main target of malware attacks. Platforms which use for example Linux or Apple operating systems are currently targeted to a lesser extent.

("OEMs") or Value Added Resellers in the enterprise market ("VARs") may be involved in the decisions which CPUs to use and which security solution to install.

22. The products of Intel and McAfee are therefore also from a commercial point of view in closely related markets.

B. CPUs

1. The relevant product markets

23. The notifying party claims that the relevant product market comprises general-purpose CPUs for servers, desktops, notebooks, netbooks, nettops, and tablets.

24. Within this scope of devices, according to the notifying party, the relevant market for CPUs should include non-x86 CPUs because in particular competition between the x86 CPU architecture and the ARM CPU architecture is intensifying. But it indicates that a narrower CPUs market definition according to the type of platform or the type of architecture does not affect market shares in a significant manner and therefore does not change the assessment.

25. In the 2009 Commission Intel antitrust decision[11] the Commission found that (1) there is a distinct market for x86 CPUs and that (2) CPUs for non-computer devices and CPUs for computers are not demand-side substitutes.

26. The Commission has also envisaged at the time a possible sub-segmentation according to the type of platform (servers, desktops and notebooks):

27. In the 2009 Commission Intel antitrust decision, the Commission has considered that a chain of substitution could exist on the demand-side across the three different types of platform, meaning that all CPUs for computers are in one relevant product market "*even though, for example, the cheapest CPUs destined for low-end desktops are not direct substitutes for more expensive CPUs destined for expensive servers*"[12]. The Commission has however ultimately left open the exact delimitation of the relevant product markets for x86 CPUs with regards to the type of platform.

28. Almost all respondents to the Commission's phase I market investigation ('the market investigation') confirm a separate market for x86 architecture CPUs as identified in the 2009 Commission Intel antitrust decision[13].

29. The market investigation suggests that it might possibly be appropriate to further segment x86 CPUs according to the type of platforms. In this regard, x86 CPUs for servers, desktops and notebooks might belong to separate product markets. X86 CPUs for new types of devices, such as netbooks, tablets, handheld devices and consumer electronics might also form different product markets that have not been assessed at the time of the 2009 Commission Intel antitrust decision. The question of further

11 See paragraphs 808 and 813.

12 See paragraph 799.

13 10 out of 13 respondents to this question.

segmentation according to the type of device can however be left open since the conclusions of the assessment remain unchanged.

30. The Commission therefore concludes that the relevant product market encompasses x86 CPUs, potentially segmented according to the type of platform.

2. The relevant geographic market

31. In the 2009 Commission Intel antitrust decision[14], the Commission concluded that the markets for x86 CPUs are worldwide. This conclusion was supported by the fact that the main suppliers compete globally, CPU architectures are the same around the world, the main customers (in particular the OEMs) operate on a worldwide basis, and the cost of shipping CPUs around the world is low compared to their cost of manufacture.

32. The market investigation confirms the notifying party's point of view that the relevant geographic markets for x86 CPUs are indeed worldwide.

33. The Commission therefore concludes that the relevant x86 CPU market has a worldwide geographic scope.

C. Chipsets

1. The relevant product market

34. Chipsets could constitute a distinct product market from other hardware components, in particular CPUs, since they can be bought and sold independently. Until a few years ago there were a number of independent chipset producers competing to produce chipsets for the x86 CPUs of Intel and AMD.

35. Apparently as a result of a number of more recent changes first in Intel's and then in AMD's interoperability policies industry analysts describe today a situation where x86 chipset markets may have to be further subdivided in the markets for chipsets compatible with Intel CPUs and chipsets compatible with AMD CPUs[15]. Intel and AMD manufacture chipset for their own CPUs only, which would support this further subdivision into two separate 'aftermarkets'. Intel, AMD and Nvidia are the sole remaining significant players on this market or markets (see paragraphs 60 and 61 below).

36. For the purpose of the present assessment, the market definition can however be left open since the conclusions of the assessment remain unchanged.

2. The relevant geographic market

37. Based on industry analyst reports, that have not been contradicted by the market investigation, the Commission considers that the market for chipsets which has very similar characteristics as the CPU market is worldwide.

---

14 See paragraph 836.

15 Mercury Research, PC Processors and Chipsets - Updated Edition 1Q2010 - Market Strategy and Forecast Report.

D. Security software

1. The relevant product market

38. The notifying party claims that within the broad IT security solutions sector, endpoint security products and services ("endpoint security") form a relevant product market where McAfee achieves three quarters of its revenue.

39. According to this IDC taxonomy, within the general category 'Secure Content and Threat Management' ("SCTM")[16], endpoint security forms a distinct product market from network security, messaging security and web security.

40. Endpoint security encompasses products that are designed to protect endpoints from attack or to directly protect information residing on endpoints. Endpoint security is generally defined as "*client antivirus products, file/storage server antivirus, client antispyware products, personal firewall products, host intrusion prevention products, file/disk encryption, and endpoint information protection and control products* […]"[17].

41. The notifying party considers also that it would be conceivable to extend the relevant market to include messaging security[18] and web security[19] because McAfee's endpoint security business unit also applies these products to some end-consumers and enterprise customers. This would illustrate the fact that there is a growing demand for the purchase of multiple security tools as a single solution.

42. The notifying party however indicates that the broadening of the endpoint security market to messaging and web security would not alter the assessment of the transaction given McAfee's limited sales of these types of security products.

43. In a previous decision[20] the Commission used similar IDC break-down general security software categories into sub-categories.

44. In this decision, the Commission also considered two potential sub-segmentations of the product market according to (i) their availability for the various OS platforms and (ii) the category of customer. The market investigation carried out by the Commission at the time did not clearly conclude that these two sub-segmentations were relevant for this

---

16 IDC describes the SCTM category as including products that "defend against viruses, spyware, spam, hackers, intrusions and the unauthorized use or disclosure or confidential information. Products in this market are offered as standalone software, software married to dedicated appliances, and hosted software services."

17 IDC – Market analysis, Worldwide Endpoint Security 2009-2013 Forecast and 2008 Vendor Shares.

18 IDC defines messaging security as including "antispam, antimalware, content filtering, and data loss prevention".

19 IDC defines web security as including "web filtering, web antimalware, web application firewall, web 2.0 security, and web data loss prevention".

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

type of security product and the Commission left the exact definition of the relevant product markets open.

45. The market investigation in the present case largely confirms that the IDC segmentation of the security solution market is appropriate[21] and that endpoint security can be regarded as a distinct product market.

46. The market investigation also suggests that endpoint security may have to be further segmented according to the type of end-user, i.e. endpoint security for consumers and endpoint security for enterprises[22]. Consumers comprise final-end users as well as small and medium size enterprises ("SMEs") whose demand characteristics and buying patterns are similar. Enterprises comprise large private companies and government bodies.

47. Consumers are often not able or willing to exactly compare the effectiveness of different security solutions. They are also less sensitive to the need to make secure use of their IT devices compared to enterprises. Both points are illustrated by the relatively important use of freemium[23] security solutions by consumers. According to a McAfee internal document, [40-50]% of consumer security users worldwide use free products[24].

48. Enterprises by contrast require high-level technologies, a broad compatibility of the security software with their potentially very diverse installed base of hardware and software. They also seek suppliers which provide a broad range of products, associated services and support. They are seeking suppliers with recognised brands which are likely to continue for a number of years to provide best of breed and state of the art technology.

49. This segmentation is supported by an IDC market analysis according to which endpoint security market "*is segmented into* […] *products that are purchased by consumers and* […] [products] *that are acquired by corporations and other organizations*"[25].

50. The Commission considers that endpoint security constitutes a relevant product market which might be further segmented according to the type of end-customers, i.e. in a market for endpoint security for consumers and a market for endpoint security for enterprises.

51. The exact definition of the relevant product markets for endpoint security can be left open, as the conclusions of the assessment would be the same regardless of whether the market for endpoint security is further segmented or extended as suggested above.

---

21 22 out of 23 respondents to this question.

22 19 out of 25 respondents to this question.

23 Freemium is as a business model that works by offering a basic product or service free of charge while charging a premium for advanced features, functionality, or related products and services.

24 McAfee presentation to DG Competition, 8 October 2010.

25 IDC – Market analysis, Worldwide Endpoint Security 2009-2013 Forecast and 2008 Vendor Shares.

2. The relevant geographic market

52. The notifying party claims that the geographic market for endpoint security is worldwide or at least EEA-wide in scope. It refers to a previous decision[26] in which the Commission has noted that suppliers offer their security software products "*globally in one standard function version, except for the language*". In this decision, the Commission also mentioned the fact that the sales prices for security software products are largely harmonized within the EEA in the sense that "*the price is set by the US/English version of the product and a premium is added to recover cost from providing the product in various languages*"[27].

53. The Commission however left open the exact definition of the relevant geographic markets for security software. It noted in particular that although larger organisations have a tendency to prefer global sourcing of security software products, small organisations or consumers could consider sourcing via alternative sales channels, within their country.

54. The market investigation confirms that the relevant geographic markets for endpoint security are at least EEA-wide.

55. In conclusion, the Commission considers that the endpoint security markets have a worldwide or at least EEA-wide geographic scope.

V. ASSESSMENT

A. Competitive landscape

1. Intel's dominant position

X86 CPUs

56. In the 2009 Commission Intel antitrust decision[28], the Commission concluded that at least between October 2002 and December 2007, Intel held a dominant position in the market(s) for x86 CPUs. The Commission indicated that Intel consistently held very high market shares in excess of or around 80% in an overall x86 CPU market and in excess or around 70% in any of the sub-markets defined according to the type of platform (servers, desktops and notebooks).

57. A vast majority of the respondents to the market investigation consider that Intel is still dominant in the overall x86 CPU market or separate sub-markets for x86 CPUs for servers, for desktops and for laptops and that the factors that led the Commission in its antitrust case to consider Intel dominant in these markets are still valid today[29]. These

---

26 Commission decision n°COMP/M.3697 – Symantec / Veritas, 15 March 2005 paragraph 18.

27 Commission decision n°COMP/M.3697 – Symantec / Veritas, 15 March 2005 paragraph 19.

28 See paragraph 912.

29 18 out of 23 respondents to this question.

factors are persistently very high market shares as well as high barriers to entry and expansion in these markets (see paragraphs 91-96 below).

58. Mercury Research estimates Intel's market share in volume for x86 CPUs in 2009 at [80-90]% worldwide. For each type of platform, including netbooks, Intel's market shares in volume for x86 CPUs in 2009 exceed [70-80]% worldwide[30].

59. With regard to the other new types of platforms (such as tablets, handheld devices, and consumer electronics), Intel is not yet active or has relatively limited market shares.

Chipsets

60. With regard to the chipsets markets, Intel's worldwide market shares in volume are very high, as illustrated in the table below.

Total Chip Sets	2009 Q4 Current Quarter		2009 Q3 Prior Quarter	
	Units	Share	Units	Share
Intel	[…]	[70-80]%	[…]	[70-80]%
AMD	[…]	[10-20]%	[…]	[10-20]%
Nvidia	[…]	[10-20]%	[…]	[10-20]%
SIS	[…]	[0-5]%	[…]	[0-5]%
VIA	[…]	[0-5]%	[…]	[0-5]%
ServerWorks	[…]	[0-5]%	[…]	[0-5]%
Total	[100-110]	100%	[100-110]	100%

(*source: Mercury Research*)

61. Intel has also gained an even higher share in the possible 'aftermarket' of chipsets for Intel x86 CPUs. As a consequence of a change of interoperability policies other chipset producers for Intel CPUs have largely exited the market.

Intel P4 Bus Chip Sets	2009 Q4 Current Quarter	
	Units	Share
Intel	[…]	[90-100]%
Nvidia	[…]	[5-10]%
SIS	[…]	[0-5]%
AMD	[…]	[0-5]%
VIA	[…]	[0-5]%
Others	[…]	[0-5]%
Total	[80-90]	100%

(*source: Mercury Research*)

30 For servers: [90-100]%; for desktops: [70-80]%; for notebooks and netbooks: [80-90]%.

Conclusion

62. Given the persistently very high market shares which are often higher than [70-80]% as well as very high barriers to entry and expansion in these markets (see paragraphs 91-96 below), the Commission concludes that Intel still holds today a dominant position in the market for in x86 CPUs whatever its segmentation, except for new platforms such as tablets, handheld devices and consumer electronics. *Prima facie* Intel appears also to be dominant in the chipsets market in particular in a possible market for chipsets for Intel x86 CPUs.

2. McAfee's position

63. McAfee is one of the few security technology companies active in practically all areas of the security technology spectrum. It serves a wide scope of customers: end-consumers, SMEs, and large private corporations and governmental organisations.

64. McAfee achieves however around […] of its total software security revenue in endpoint security where it is worldwide the number two player measured by revenue ([10-20]%) behind the leader Symantec ([30-40]%). McAfee's worldwide endpoint security sales represented about USD […] million in 2009.

65. While McAfee's EU revenues in the consumer segment (USD […] million) are considerably lower than in the corporate segment (USD […] million), the opposite is true in the US (USD […] million, compared to USD […] million).

66. In both segments, McAfee remains number two, behind Symantec (see paragraphs 74-82 below).

67. Should an EEA-wide geographic market be assessed, McAfee's positions are not significantly different.

68. On the other markets of security software (network, messaging, web security, identity access and management, security and vulnerability management), McAfee's positions are limited. Based on an Intel internal document based itself on IDC studies[31], McAfee's worldwide market shares in 2009 on these markets can be estimated as follow:

Network	[0-5]%
Messaging	[5-10]%
Web security	[0-5]%
Identity access and management	Not active
Security / vulnerability management	[0-5]%
Other	[0-5]%

31 Intel Presentation to DG Competition, 2 September 2010.

3. The parties' competitors

3.1. CPUs and chipsets markets

CPUs

69. While the x86 architecture with Intel and AMD as the main producers remains pervasive for servers, desktops, laptops and netbooks, this architecture faces some competition in netbooks and very strong competition in handhelds from ARM, a company that has developed a RISC architecture used in most mobile devices such as smartphones.

70. ARM is built on the basis of a RISC architecture developed by ARM Holdings. Whereas ARM CPUs were originally conceived as CPUs for desktop personal computers, their relative simplicity made them particularly suitable for low power applications. ARM architecture is currently the most widely used for mobile and embedded electronics applications. However, it currently does not support Microsoft's operating system ("OS") Windows, which limits its footprint in the desktop and laptop segments[32].

71. The x86 architecture today also faces a limited degree of competition from graphic cards manufacturers (e.g. Nvidia). A GP-GPU (General Purpose Graphic Processing Unit) can indeed to a certain extent perform the same functions as a standard CPU. In particular, a GP-GPU can handle more computing tasks and, consequently, it may reduce the demand for high-end CPUs.

72. In the competitive landscape in the overall x86 CPU market, Intel takes a prominent position with over [80-90]% of the market share of the volume shipped. AMD holds a much lower share of the market, while Via's position is insignificant in terms of volume shipped. The table below presents Intel competitors' market shares.

Overall x86 CPU Share	2009 Q4 Current Quarter		2009 Q3 Prior Quarter	
	Units	Share	Units	Share
Intel	[…]	[80-90]%	[…]	[80-90]%
AMD	[…]	[10-20]%	[…]	[10-20]%
VIA	[…]	[0-5]%	[…]	[0-5]%
Total	[110-110]	100%	[90-100]	100%

32 In the course of the Commission' investigation, Microsoft has announced that the next version of Windows will support system on chip architectures from Intel, AMD, and ARM. See its press release: http://www.microsoft.com/presspass/press/2011/jan11/01-05SOCsupport.mspx.

Chipsets

73. According to an industry analyst[33], the market for chipsets has been highly competitive until recently: a radical shift took place in the 2008-2009 timeframe, as a result of market consolidation and technological developments. Consequently, the number of market participants that is shipping significant volumes of chipsets has decreased from seven in 2005, to three in the current market situation, two of which are also supplying CPUs (Intel and AMD)[34].

3.2. Endpoint security

74. According to IDC[35], worldwide revenue for the endpoint security market reached USD [6000-7000] million in 2008[36]. The consumer market (USD [3500-4000] million) is larger than the corporate market (USD [2500-3000] million) but this latter is foreseen to grow at a faster pace within the coming years.

75. On the overall worldwide market for endpoint security, the market shares of McAfee and its main competitors are the following:

---

33 Mercury Research, PC Processors and Chipsets - Updated Edition 1Q2010 - Market Strategy and Forecast Report.

34 See paragraphs 60 and 61 above.

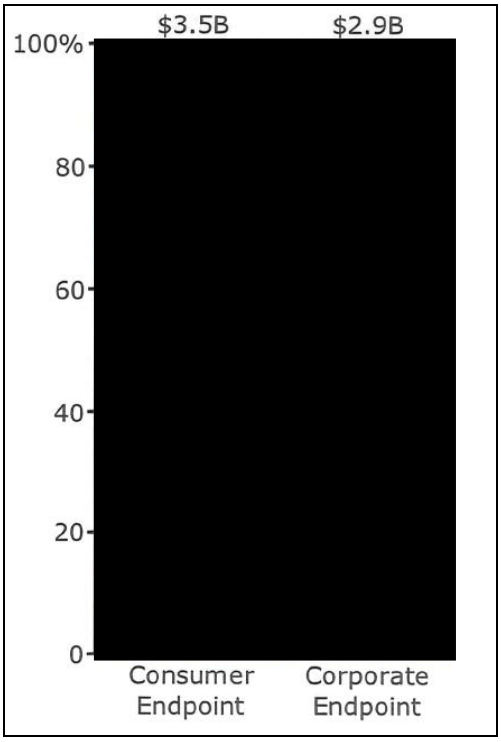
35 Almost all respondents to the market investigation consider that the market shares in the security solutions market in terms of revenue which are published by the industry analyst IDC are a good reflection of SSVs' competitive position.

36 IDC – Worldwide Endpoint security 2009-2013 Forecast and 2008 Vendor shares.

Security Software Vendor	2008 turnover (USD million)	2008 market share
Symantec	[…]	[30-40]%
McAfee	[…]	[10-20]%
Trend Micro	[…]	[5-10]%
Kaspersky Lab	[…]	[0-5]%
Sophos	[…]	[0-5]%
AVG Technologies	[…]	[0-5]%
F-Secure Corp.	[…]	[0-5]%
BitDefender	[…]	[0-5]%
Panda Software	[…]	[0-5]%
Check Point	[…]	[0-5]%
Others	[…]	[10-20]%

Source : IDC. Revenue covers all security products but excludes earnings from professional services such as consulting, implementation, operations, education and training.

76. Symantec is the leader of this overall market, followed by McAfee and Trend Micro. These three companies are the only ones mainly active in both the endpoint security for consumers and in the endpoint security for enterprises, as illustrated in the graphic below.



Source: Intel internal document based on IDC studies[37]

Endpoint security for consumers

77. The two main competitors of McAfee in this market are Symantec and Trend Micro. Together these 'three big vendors' have the largest R&D budgets. They account for over [70-80]% of revenues in endpoint security for consumers[38] and play a pivotal role in the broader security software market. They also have the closest technological and commercial relationships with CPU vendors ([…]), OS vendors (in particular Microsoft) and OEMs. Only Symantec, McAfee and Trend Micro are to a commercially significant extent active in the OEM channel, i.e. have agreements with OEMs to preinstall their security software for a free trial and possible later conversion on the computers shipped by the OEMs in question.

78. Besides the three big vendors, there is a large number of smaller often regional endpoint security vendors such as Kaspersky, F-Secure, AVG, Avast, Avira, or Panda Security.

79. In the consumer space many of those smaller players operate on the basis of a freemium business model and offer their basic security software for free. Their deployment shares are thus often much more important than the revenue market shares suggest. According to a McAfee's internal document, [40-50]% of consumer security users worldwide use free product offerings provided by 31 companies[39]. The current 'freemium' leaders are AVG, Avast and Avira that claim, according to this internal document, "more than 100 million users". Microsoft has also free security product offerings for consumers.

---

37 Intel Presentation to DG Competition, 2 September 2010.

38 IDC Market Analysis "Worldwide Endpoint Security 2009-2013 Forecast and 2008 Vendor Shares".

39 McAfee presentation to DG Competition , 8 October 2010.

Endpoint security for enterprises

80. According to Gartner[40], this market is "*still dominated by the market share of the big-three traditional antivirus vendors – McAfee, Symantec and Trend Micro – which, together, represent roughly 85% of the market share*". Gartner notes also that "*many nimble vendors are beginning to challenge the status quo with innovative endpoint platforms solutions and a higher level of customer focus*". However, "*despite the introduction of new players, the displacement of incumbents is still a significant challenge. The biggest impact for the challengers and visionaries is to push the dominant market players into investing in new features and functionally, and to keep pricing rational*"[41].

81. According to an Intel Presentation to DG Competition[42], from which the above graphic is extracted, McAfee ([10-20]%) competes with Symantec ([20-30]%), Trend Micro ([5-10]%), but also Sophos ([5-10]%), Cisco ([0-5]%), IBM ([0-5]%), CA ([0-5]%), Check Point ([0-5]%) and other competitors that together represent [30-40]% of this market.

82. Although, given the differences in the data from Gartner and IDC, it was not possible during the phase I investigation to establish fully reliable market shares for corporate endpoint vendors, the Commission considers that McAfee, Symantec and to a lesser extent Trend Micro are the three main competitors in endpoint security for enterprises, in particular for the largest enterprises. Sophos' market share in large enterprises remains limited compared to Symantec's, McAfee's and Trend Micro's. Thus, according to Gartner, "*Sophos is continuously challenged to differentiate itself from the 'big three' players* […]"[43].[…]The same analysis applies to the remaining even smaller competitors.

4. The parties' customers

4.1. Intel's customers

83. OEMs are the main direct customers for CPUs and chipsets. Intel sells directly to the 11 largest OEMs[44] which represent about […] of Intel's sales. These multi-national corporations negotiate with Intel for their worldwide purchases from the site of their corporate headquarters. Intel negotiates price framework agreements that typically last […]. Some negotiations for systems directed at enterprises (both PCs and servers) may however have a […] cycle and additional agreements can be negotiated for shorter periods when they are linked to specific sales events, such as 'back-to-school' or 'holidays season' sales activities, or in the context of bidding events organized by the

40 Gartner – Magic Quadrant for Endpoint Protection Platforms, 4 May 2009.

41 Gartner – Magic Quadrant for Endpoint Protection Platforms, 4 May 2009.

42 Case M.5984 – Intel / McAfee – Presentation to DG COMP, 'Competitive landscape', p.3. Data used by Intel are extracted from IDC study Worldwide Endpoint Security 2009-2013 Forecast and 2008 Vendor Shares.

43 Gartner – Magic Quadrant for Endpoint Protection Platforms, 4 May 2009.

44 These customers are in alphabetical order: Acer, Apple, Asustek, Dell, Fujitsu, HP, IBM, Lenovo, Samsung, Sony and Toshiba.

OEMs for their enterprise clients. OEMs typically refresh their existing product offerings and launch new designs in regular cycles (three or four times per year).

84. Regional OEMs[45] account for about […] of Intel's sales. They buy CPUs and chipsets directly from Intel. According to Intel, the list prices and discounts negotiated with these customers tend to follow the same pattern as those that are negotiated with the large multi-national OEMs.

85. Intel also sells indirectly to more than […] local OEMs that operate in the so-called 'white box channel'. They represent the remaining […] of Intel's sales. These are Intel's indirect customers. Local OEMs buy from independent distributors that have been appointed by Intel as its non-exclusive resellers usually for a period of […]. Intel publishes recommended list prices for its distributors about three to four times a year.

4.2. McAfee's customers

86. McAfee develops products and services for enterprises (including governments) and consumers (including SMEs).

87. In the enterprise segment, about […] of McAfee's sales are generated through value-added resellers ("VARs") and systems integrators ("SIs"), who install and configure the products and may also manage the system. The remainder of McAfee's sales in the enterprise segment ([…]) are made directly by McAfee's sales force.

88. In the consumer segment (including SMEs), about […] of McAfee revenues are generated through the OEM sales channel. OEMs operate as a distribution partner for McAfee and pre-install security products on their PCs for a fee. Consumers have the opportunity to use them for a limited trial period (typically 30, 60 or 90 days) before having to pay a subscription fee to receive updates for protection against new malware. According to Intel, when choosing an SSV partner, OEMs consider the financial terms they offer, their brand and their ability to provide support once products ship. McAfee's OEM partners currently include Acer, Dell, HP, Lenovo, Samsung, and Toshiba.

89. Internet Service Providers ("ISPs") represent about […] of McAfee's revenue in the consumer segment. McAfee's ISP partners currently include ATT, BT, Telefonica, Comcast, Verizon, Telstra, Big Globe, China Unicom and Singtel. The ISP may either charge subscribers for the added security protection service or provide it for free. The ISPs are generally charged either on a per-subscriber or on a flat rate basis. If the end-users pay a fee to the ISP for the use of the security product, McAfee will normally receive a share of this revenue. Where the end-user receives the service for free, the ISP typically pays McAfee.

90. The retail channel[46] represents around […]% of McAfee's revenue in the consumer segment. About […]% of McAfee's revenue in the consumer segment is directly generated through sales made from its website.

---

45 According to Intel terminology, regional OEMs are large but regional OEMs that buy directly from Intel.

46 The retail channel concerns the sales of physical boxes of security software.

5. Markets characteristics

5.1. CPUs and chipsets

Barriers to expansion and entry

91. In the Commission 2009 Intel antitrust decision, the Commission indicated that a potential entrant faces significant intellectual property barriers and has to engage in substantial initial research and development and production investment to be able to start production of x86 CPUs[47].

92. Moreover, once this investment has been made, it is necessary to achieve a high capacity utilisation to minimise average cost and thus compete most efficiently with the incumbent manufacturers already in the market (essentially, Intel and AMD)[48].

93. Therefore, in the light of (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, the Commission concluded that there are significant barriers to entry in the CPUs market.

94. Furthermore, once entry has taken place, a manufacturer's production capacity is limited by the size of the existing facilities. Expanding output requires additional investment into new property, plant and equipment as well as several years lead time.

95. Intel however pointed out the entry in the market of CPUs of several companies who obtained licenses from ARM Holdings for its CPU core and then developed and launched derivative designs based on the licensed core.

96. The market investigation confirms the findings made in the Commission 2009 Intel antitrust decision, in particular the Commission analysis of the barriers to expansion and entry which are still high. A respondent to the market investigation explains that this can be explained by the critical mass of products which have to be sold due to previous high development and manufacturing costs[49].

Innovation

97. In the Commission 2009 Intel antitrust decision, the Commission underlined that innovation is, together with price, one of the main factors that triggers demand in the x86 industry. The very high research and development ("R&D") and production costs can usually only be recovered if new inventions can be sold before the competitor

---

47 See paragraph 866.

48 The "fabless" model, mentioned in paragraph 11, meaning that a player does not have any production or manufacturing facilities, but instead subcontracts the manufacture of its products to third party fabs, could be a mean to limit entry costs. But this model is not widespread in the CPU markets that remain dominated by the only integrated manufacturer, Intel.

49 Non-Confidential response to the Commission's market investigation.

responds with a more innovative product. The pace of innovation is rapid, which means rapid increases in CPU transistor density and rapid improvements in the CPU architecture.

98. According to Intel, it has indeed to improve regularly its product design and production technology. In particular, Intel's R&D efforts focus on increasing the functionality of its CPUs by incorporating additional features.

99. CPU transistor density generally doubles about every eighteen months. For CPU producers, this is mainly relevant when it comes to investment in new and more innovative production facilities which manufacture dies with increasingly smaller circuitry. Transistor density also has an impact on the performance of the CPU.

5.2. Endpoint security

Barriers to expansion and entry

100. According to the market investigation, barriers to entry seem to be relatively low for small players. In the consumer market, it appears not so difficult to become either a specialist niche player or an imitator, employing the freemium model.

101. In contrast, barriers to expansion both in the enterprise and the consumer segment seem to be significant.

102. In the enterprise segment, the key factors mentioned in the market investigation were brand recognition, range of products, services and support, and trust that the company will continue to innovate. Some respondents to the market investigation mention in particular the necessity to have a widespread threat detection system and a threat intelligence database in order to compete effectively. Currently, only a few number of SSVs maintain their own global threat detection.

103. Economies of scale are essential to support the R&D and infrastructure necessary to provide today’s advanced security services. Security software has to be updated continuously with the latest malware alerts to provide effective security. Providing these updates requires an extensive infrastructure. Only the larger security vendors can detect new malware quickly and provide the appropriate level of preventative service demanded by customers.

104. In the consumer segment there is a clear division between the players with access to the OEM channel (Symantec, McAfee and Trend Micro) and the other players, mainly the freemium players, without such access.

105. Symantec, McAfee and Trend Micro have built high brand recognition and have high revenues with relatively low penetration.

106. Moreover, these players benefit from network effects that increase the barriers to expansion. Indeed, the more users an SSV has, the higher its chances to detect new malware, in particular when those users are distributed evenly across different geographic areas.

107. Symantec, McAfee and Trend Micro have high R&D budgets and global threat detection networks.

108. On the contrary, these characteristics are less important for the freemium players that lack access to the OEM channel. These players are generally characterized by high market penetration, a lower R&D budget and relatively low revenues.

Innovation

109. The security market is globally characterized by rapid innovation.

110. SSVs have indeed to invest in innovation given the intense competition in these markets. According to Intel, the R&D budgets associated with finding specific set of malware samples, processing those samples and enhancing the software security products are largely similar among SSVs regardless of their size. But Intel justifies the higher R&D budgets for companies like McAfee and Symantec by the necessity to support larger product portfolios and larger customer bases. According to Intel, SSVs with smaller R&D budgets are able to effectively compete by concentrating their efforts on narrower product portfolios and focusing on specific customer segments and/or security threats.

111. Intel's argument is however contradicted by one McAfee's competitor, according to which "[…] *while it is acknowledged that currently some security software providers succeed in bringing a competitive product to market on the basis of limited R&D programs, these companies tend to be focused on a narrow set of applications. They consequently lack the same breadth of coverage as McAfee, Symantec or others. For this reason and given their less stable position in the market, these start-ups will typically not be considered viable suppliers to enterprise customers*"[50].

112. The market investigation shows generally that significant and continuous innovation is indispensable to effective security[51].

5.3. Relationships between CPUs/chipsets manufacturers and endpoint security vendors

113. Historically, Intel has regularly briefed SSVs on new and upcoming CPUs and chipset features. It has also provided libraries for common features optimised for new products. It has made available tools and consulting to enable SSVs to optimally use the CPUs/chipsets. It has actively sought feedback from the SSVs community on future features.

114. Intel has several different models of cooperating with software vendors: (1) high-touch; (2) mid-touch; and (3) scale partners.

115. High-touch accounts consist mainly of Microsoft and Symantec for whom Intel typically dedicates account managers and engineers to service these accounts. Intel works with these accounts earlier in the process because of their larger scale and expertise to understand what feature sets will be useful to the software development community.

---

50 Non-Confidential response to the Commission's request for information of 16 December 2010.

51 9 out of 12 respondents to this question.

116. Mid-touch accounts receive, according to Intel, slightly less personalization than high-touch accounts, with managers and engineers dedicated across many different software vendors. These accounts typically represent mid-sized software vendors who have less scale and resources to commit developments efforts. They are also invited to participate in validation efforts prior to launch, though typically closer to the launch date when the product is more developed. The majority of SSVs such as McAfee, Trend Micro and Kaspersky fall into this category.

117. The scale partners are the smaller SSVs who use the Intel Software Partnership Program ("ISPP"). This program distributes materials to the scale partners. Information available through the program contains the same set of final technical specifications available to high and mid-touch accounts and provides any SSVs with the key information it needs to adopt Intel features in its software.

118. Intel has generally open dialogues with many SSVs during development of new products.

119. Although the product roadmaps for hardware and software are not typically aligned to facilitate input into a new roadmap[52], Intel has carried out a general method of collaboration with software vendors (including SSVs), as described in the following table:

Timeline	**Type of collaboration**
Three to five years before product launch	High level discussions with a few selected SSVs – […]
Twelve to eighteen months before product launch	For those features that may lead to product development, Intel contacts an increasing number of SSVs. […]
Six to twelve months before product launch	[…]. Early validation of the [Intel hardware] features with some vendors.
Three months before product launch	Intel expands its validation efforts to include a broader set of vendors.
Product launch	In most cases, full technical details about a new feature are made available to all software vendors via the ISPP.

52 Intel's product cycle for new hardware is generally around five years whereas software development generally occurs on a six to twelve month timeline.

B. Competitive assessment

1. Introduction

120. Although there is no relevant horizontal overlap or vertical relationship between Intel and McAfee, the Commission considers that their respective products are largely complementary and closely related[53]. The transaction may therefore give rise to conglomerate effects.

121. In most circumstances, conglomerate mergers do not give rise to competition problems[54]. In some cases, in particular where as in the present case the merged entity enjoys strong market power in at least one of the markets concerned, a conglomerate merger may however create possibilities for exclusionary bundling or tying practices that could disadvantage or foreclose competitors and ultimately lead to them exiting the market, or otherwise significantly impede competition in the markets concerned.

122. Following the proposed transaction, Intel will have the ability to offer both hardware (in particular CPUs) and security solutions. As a result, the Commission investigated whether there was a serious risk that Intel would bundle or tie Intel CPUs/chipsets and McAfee security solutions.

123. The Commission's following assessment is based on submissions made by several complainants, mainly McAfee competitors, but also submissions made by other market participants (competitors of Intel in hardware markets, competitors of McAfee in security software markets and customers of both Intel and McAfee), submissions made by third party market observers and internal documents of both Intel and McAfee obtained in the course of the investigation.

124. The complainants consider that it is likely that post transaction the parties will engage in three main types of practices, namely degradation of interoperability between Intel's hardware and security solutions on the one hand and the products of competitors on the other (see section 2 below), technical bundling/tying ("technical tying") (section 3) and commercial bundling strategies (section 4). The Commission has also assessed a possible combination of commercial bundling together with technical tying or a degradation of interoperability (section 5).

125. Such business strategies would aim to leverage Intel's dominance in the CPU and chipset markets into the endpoint security markets, leading to the exit or at least significant weakening of McAfee's main competitors within the next two to five years. Complainants are in particular concerned that the ensuing Intel/McAfee security monoculture would reduce competition and innovation in the endpoint security markets with significant consequences for overall security of computing devices in general.

126. For each of these practices (degradation of interoperability, technical tying, commercial bundling, and a combination of such practices), the Commission assessed the three issues identified in the EC non-horizontal merger guidelines: (1) ability to

---

53 See paragraphs 18-22 above.

54 Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings ("EC non-horizontal mergers guidelines"), paragraph 92.

foreclose, (2) incentives to foreclose, and (3) the overall likely impact on competition and consumers[55].

127. For the sake of clarity, antitrust rules, in particular article 102 TFEU will continue to apply to the merged entity after the closing of the proposed transaction, regardless of the outcome of the present assessment under the Merger Regulation.

2. Assessment of a foreclosure strategy based on degraded interoperability

128. For the purpose of the present decision, interoperability can be defined as the possibility for software and hardware to interact[56]. 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.

129. According to the complainants a degradation of interoperability would affect the ability of SSVs to develop or optimise their products, notably, with regard to the use of power and the performance of the security solutions.

130. In particular, Intel could keep undisclosed certain parameters (such as performance related parameters, side effects of the use of instructions on CPU and memory state) and reserve those for exclusive use by McAfee. This would result in McAfee being able to develop better security solutions within less time than its competitors.

131. Moreover, Intel could optimise the interfaces (application programming interfaces – "APIs") between its chipsets/CPUs and McAfee's security solutions, its compilers[57] or its software development kits[58] ("SDKs") according to McAfee's design preferences, while

---

55 Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings ("EC non-horizontal mergers guidelines"), paragraph 94.

56 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:2009:111:0016:01:EN:HTML

57 A compiler is a computer program (or set of programs) that transforms source code written in a programming language into another computer language. A complier is primarily used for programs that translate source code from a high-level programming language to a lower level language (e.g., assembly language or machine code).

58 SDK is typically a set of development tools that allows for the creation of applications for a certain software package, software framework, hardware platform, computer system, video game console, OS, or similar platform.

the integration with the solutions of competing SSVs would be altered. This would result in McAfee's security solutions running better on Intel's CPUs than the endpoint security of the other vendors.

2.1. Ability of Intel to degrade interoperability

The notifying party's view

132. Intel considers it has no ability to foreclose on the basis of a degraded interoperability.

133. First, Intel claims that it cannot technically hamper the interoperability of its products because new instruction sets of a CPU are made accessible to SSVs through a series of interconnected system software layers provided by third parties (such as vendors of BIOS, virtual machine monitors or OS). Once an instruction is visible to any application software, it can be easily seen and used by others.

134. Second, Intel argues that it would be impossible to permanently hide instructions, as it would be easy for third parties to detect and reverse engineer them (via debuggers, compilers, etc.).

135. Third, according to Intel, SSVs do not write software to directly use such instructions. SSVs typically write their software at a high level of abstraction and let compilers adjust the code for the specificities of a CPU. In many cases, the OS also consolidates multiple hardware features into software functions that are easier to use and allow software to access these functions through APIs.

136. Fourth, according to Intel, the delay in revealing new instruction sets until release would not provide McAfee with any sustained advantage. The penetration of any new McAfee software using such instructions would be limited absent an installed base of CPUs containing the new instruction set.

137. Fifth, the current instructions sets are publicly disclosed. There would be no way to disable or affect instruction sets that are already in use since part of the benefit of the x86 architecture is its backward compatibility (new CPUs continue to support old instruction sets).

138. Intel has mandated two IT experts to provide the Commission with reports that support these arguments[59].

Results of the market investigation

139. The market investigation generally indicates that Intel has the ability to favour McAfee's interoperability with its hardware and thereby to degrade interoperability between its hardware components and the solutions of McAfee's competitors.

140. First, the market investigation indicates that software developers need a range of information (documentation on the CPU instructions, roadmap of developments at the

---

[59] Report on the Implications for Microprocessor Design following an Intel-McAfee Merger by Dr. Gregory Papadopoulos and Expert report of Mr. Nathan A. Brookwood.

CPU level) and a number of tools (interfaces, compilers, SDKs) from the CPU manufacturers to develop and optimize their software for a given CPU. This appears to be particularly the case for security solutions, which operate closer to the CPU than most software and for which the information would become even more crucial in the future when security solutions are likely to interact more closely with hardware components than today. Such an anticipation is shared by McAfee in publicly disclosed statements[60].

141. Second, while the market investigation generally confirms that Intel currently generally discloses and documents the CPU instructions, and cooperates with software developers in an open manner, they indicate that post merger Intel, by hiding certain instructions in the CPU, limiting or delaying the information available to software developers, could favour McAfee's interoperability by documenting certain features of the CPU only for McAfee. In particular, one Intel competitor indicates that: "*certain parameters could remain undisclosed. It is quite difficult to measure the behaviour of an isolated instruction in a modern CPU. Intel might accelerate a certain code sequence that performs an important function in the McAfee code. Others would be unlikely to stumble upon that particular code sequence for implementing their version of the function. Since similar code can have widely different performance on a modern CPU, even just giving McAfee programmers very good access to Intel performance engineers could greatly increase the performance of McAfee code that McAfee competitors would not have.*"[61]

142. This form of 'positive discrimination' is believed to be more realistic than a degradation or exclusion of interoperability for McAfee competitors. According to one of them, "*rather than degrading the performance of certain applications, Intel would make McAfee use better performing APIs or procedures of the CPUs. It would be a form of positive discrimination. McAfee could use the CPU to its fullest potential while the rest would not do it because they could be prevented from accessing the same level of interoperability information.*"[62] Moreover, as indicated by the same respondent to the market investigation, "*It is perfectly possible for a CPU vendor to reserve access to certain functions in the CPU to only one security vendor. It is a design choice. Hardware can be made as software agnostic or software fanatic as desired.* […] *The same instructions used by different software will be processed in the same way by the CPUs. They are software agnostic in this way. However* […], *it is perfectly possible that*

---

60 McAfee's Chief Technology Officer recently stated that: "*It is the combination of software and silicon that will create the next generation of security technology. I believe that security will follow a path similar to the one that virtualization has taken over the past decade, starting out as a proprietary application, moving to a hypervisor, and then ultimately providing a better solution through hardware-assisted technologies like Intel VT-x. Antivirus has operated as an application for 20 years, similar to the early desktop virtualization products. Just like virtualization that moved down the stack with dedicated hypervisors, security too will follow. We will be able to utilize the silicon to enable the security software and provide better performance and higher efficacy in blocking malware, which I believe will be welcomed by customers*". See: http://blogs.mcafee.com/corporate/cto/intelmcafee-security-activation-not-software-elimination.

61 Non-confidential reply to the Commission's market investigation.

62 Non-confidential reply to the Commission's market investigation.

hardware functions are unlocked only by one application or code known to only one company." [63]

143. While the market investigation indicates that selective degrading of interoperability only for SSVs would be difficult to implement, since they generally use the same instructions as other vendors, this would be feasible in a limited number of occurrences only, for instructions more directly designed for security purposes. According to one McAfee's competitor, "*such degradation would not necessarily affect non-security solutions. There are some functions that only security products typically need, such as the ability to inspect, intercept and kill[,] threads and processes. Anything that advantages McAfee in this respect would create an important advantage. Or, Intel could provide McAfee a reserved portion of cache or other parts of the CPU and not enable access to these in the SDKs and compilers. Such lack of access would have no effect on any software, but would disadvantage security ISVs trying to compete with McAfee.*"[64]

144. Although the market investigation indicates also that a degradation strategy targeted at specific competitors would probably be rapidly detected, it shows that it would be more difficult to detect a strategy favouring interoperability of McAfee with certain features of the CPU.

145. Third, contrary to what Intel claims, only a limited number of respondents to the market investigation believe that the ecosystem of security software vendors could efficiently react to discrimination as regards interoperability by reverse engineering Intel's hardware components. Most of them consider that such reverse engineering would be partial, time consuming (possibly several months if not years) and prohibitive in terms of costs. In addition, according to one OEM, "*undocumented instructions may or may not be able to be "reverse engineered". While a persistent investigator could probably discover such instructions, it would likely be difficult to determine the specific function and syntax required to effectively use them. Undocumented instructions would not be officially supported by Intel and would be subject to change in future CPU iterations. As a result, it would be risky for a third party to rely upon such undocumented instructions, even if the syntax and function were correctly determined. In addition, to the extent that elements of computer architecture are protected by patents or other IP, it may not be possible for a third party to duplicate or use such architectural elements without infringing the CPU manufacturer's patent or other IP rights*."[65]

146. This possibility is confirmed by an internal document of McAfee[66] which describes an undisclosed project for a future new product […]. Respondents to the investigation (one competitor and one expert) have also mentioned that a part of AMT can be reserved

---

63 Non-confidential reply to the Commission's market investigation.

64 Non-confidential reply to the Commission's market investigation.

65 Non-confidential reply to the Commission's market investigation.

66 […].

for McAfee to the exclusion of others[67]. There are thus no technical obstacles to a strategy of denying interoperability to others.

147. Finally, some competitors have indicated that Intel could degrade McAfee's interoperability with chipsets or CPUs other than Intel.

Results of Commission assessment

148. In view of the above, the Commission considers it likely that Intel has the ability to favour McAfee's security software interoperability with its hardware (Chipset/CPU).

2.2. Incentives of Intel to degrade interoperability

The notifying party's view

149. According to Intel, its technologies and instructions sets are generic, which means that they are used by any software vendor, not only SSVs. Because these instructions are generic, Intel would not be in a position to hide these without altering the interoperability of its CPUs with other software than security solutions, which would not be in Intel's interest.

150. Intel indeed considers that as a CPU manufacturer it has always every incentive to maintain an open software platform with a multitude of software available to consumers. Similarly, it would be in Intel’s best interest to have all software, including security software, run as efficiently as possible on its CPUs. By limiting interoperability information, Intel would make its CPUs less attractive, giving end-users and OEMs an incentive to shift away from Intel hardware.

151. This would be the reason why Intel publicly documents all the information necessary for interoperability between the CPU hardware and software (including existing security software). As a matter of practice, Intel has disclosed all necessary information to allow interoperability between software and its CPUs about a year prior to when an Intel CPU is shipped.

152. In addition to publishing the instructions, Intel would work directly with software vendors who are interested in optimizing their software specifically for the disclosed Intel features, although many are able to optimize based on their own expertise or with the help of tools such as those Intel sells on its website.

153. Finally, as mentioned in paragraphs 113-119, Intel also collaborates with various software vendors and discloses information prior to making such information publicly available under non-disclosure agreements. Disclosure of information under these agreements depends on the specific project requirements.

---

[67] A competitor states that "*Intel is able to embed McAfee software in the CPU / chipset to create, in conjunction with the vPro technologies, a McAfee security partition (running within or alongside Intel AMT).*", while an IT expert explains that "*Intel AMT is a great example of how Intel can reserve/lock down some functionality only for its own software. Intel AMT software is being kept on a flash chip on the motherboard (might not be produced by Intel), but the Intel chipset (which has recently been integrated onto the processor die, in Intel Core i5/i7 processors) verifies if the AMT code is signed with Intel digital certificate, and only then allows execution of this code on the chipset's internal processor (the 'AMT processor').*"

Results of the market investigation

154. First, several respondents to the market investigation point to the following recent statement of the CEO of Intel Paul Otellini: "*While we'll still work with the Symantecs and Microsofts and Nortons of the world, we're also going to make sure that the best possible solution is Intel on Intel or Intel on McAfee in this case and that it's architected to run best together*"[68]. Such a declaration has been interpreted as Intel's explicit intention to favour McAfee by granting it better access to Intel features or technologies than its competitors.

155. Second, the market investigation refers to […] the FTC […] subsequent order of 2 November 2010 where the FTC has required Intel [not to design] […] interfaces in a manner that restricts the ability of a GPU to interface with its CPU ("the FTC settlement case")[69]. Moreover, FTC has required Intel to disclose that Intel computer compilers discriminate between Intel CPUs and non-Intel CPUs to software developers.

156. One may argue that, contrary to the FTC settlement case, […], security software is not a potential challenge to Intel's CPU dominance. However, it is possible that the acquisition of an SSV at a significant price and subsequent ability for Intel to monetise a computer over the entire life cycle of the security software will negatively affect Intel's pre-merger incentives to partner in a neutral way with all relevant SSVs. According to one of McAfee's competitors, "*prior to the merger Intel shared information in order to encourage security vendors to innovate products supporting its hardware. Now, McAfee's competitors are directly competing with Intel through McAfee. The fact that McAfee's performance is now directly linked to Intel's performance means that it no longer makes commercial sense for Intel to continue supporting all security products equally. Such a practice would clearly be to its commercial detriment.*"[70]

157. Furthermore, Intel could have an incentive to protect its dominance on the CPU market with certain McAfee features running (in an optimal way) only on Intel platforms, which could result in creating artificially the perception that competing platforms are insecure in comparison to Intel/McAfee's offering.

158. Third, the market investigation suggests that hampering interoperability would result into gains for Intel/McAfee on the endpoint security markets. According to one of McAfee's competitor's, "*if Intel chose not to give ISVs[71] complete information and/or technically degraded the interoperability of its chips with third party products – bearing in mind that this could be achieved in a number of ways (many of which would be difficult to detect) - this would simply result in ISVs' products performing less well with Intel CPUs than McAfee security software. As noted above, robust security software is critical to any computing environment and any degradation in performance will undermine consumer confidence in (and demand for) non-Intel/McAfee products. As*

---

68 Barclays Capital Global Technology's conference, 9 December 2010.

69 Intel Corporation v The Federal Trade Commission [2009] Docket n°9341, File n°061 0247.

70 Non-confidential reply to the Commission's market investigation.

71 Independent software vendors.

above, this strategy would result in increased demand for McAfee security software, and would not result in any decrease of OEMs' Intel CPU requirements."[72]

159. Fourth, according to most respondents to the market investigation, it is very unlikely that such a strategy backfires and results in Intel losing CPU revenues. The only way CPU revenues would decrease would be if end-users show such a loyalty to an SSV other than McAfee that they would switch their demand to an alternative CPU supplier. Given the must-stock status of Intel's hardware, as acknowledged by its high market share and its brand penetration, such a scenario does not appear plausible. According to one respondent to the market investigation, "*the only way CPU revenues would decrease in this scenario would be if end-users show such a loyalty to a security vendor (other than McAfee) that they would switch their demand to an alternative CPU supplier. In practice, this would mean that a significant part of the market decides to purchase AMD CPU's, so that they can use their preferred security vendor in good conditions.* [We] *can safely rule out this possibility outside exceptional cases. Even where such an end-user loyalty would exist, resellers (including OEMs, VARs, retailers, etc) would act as an additional barrier since they often leave little choice for the end-user. Independent security vendors would be unlikely to be in a position to bend the arm of these resellers to choose against Intel.*"[73]

160. The market investigation shows that customers would not be in a position to exert pressure on Intel to restore interoperability. Moreover, they seem to consider that there is limited scope for successful counter-strategies from Intel and McAfee competitors, given in particular the limited market share of Intel's competitors. As noted by one McAfee's competitor, "*if Intel chose to completely deny any interoperability with ISVs' security software, this would ultimately be equivalent to technical tying.* […] *OEMs (customers of both Intel and McAfee) would only be in a position to switch very marginal amounts of their CPU requirements, which would not impact Intel's incentives to pursue such a strategy (and which Intel could easily offer inducements to avoid). If, alternatively, Intel chose to make information available to ISVs later than to McAfee, and/or to provide less complete information or to degrade (rather than deny) interoperability, this would result in consumers perceiving McAfee software as being more effective than other security software. As noted above, it would not be commercially viable or technically feasible for ISVs to 'reverse engineer' the McAfee software to discover the undisclosed CPU instructions or identify the reason for the degradation of their software performance.*"[74]

161. The Commission's assessment is also supported by some internal documents of the parties that indicate that Intel may have some incentives to stop its open disclosure policy with regard to security features. In particular, […][75].

---

72 Non-confidential reply to the Commission's market investigation.

73 Non-confidential reply to the Commission's market investigation.

74 Non-confidential reply to the Commission's market investigation.

75 […]

Results of Commission assessment

162. In view of the above, the Commission considers it likely that Intel has incentives to degrade interoperability of its hardware with other security solutions than McAfee's products.

2.3. Effects on markets

The notifying party's view

163. First, according to Intel, even if it had the ability and the incentive to degrade interoperability, taking such action would have a very limited effect on competition. Any hypothetical advantage Intel could give McAfee would need to be premised on a new Intel CPU, so such an action would very likely be futile given the rate of adoption of new hardware by the market. By the time a sufficient installed base of Intel hardware with the new feature existed for McAfee's product to gain any traction, every McAfee's competitor would have had more than sufficient time to come to market with a competing product.

164. Second, Intel considers that there are no features on its CPU instruction set roadmap that seem likely to be a source of sustained competitive advantage to an SSV. In addition, Intel outlines that the commercial success of security software depends not only on technical features, but on a multitude of factors, including price, and marketing.

165. Moreover, Intel submits that performance is not a source of differentiation for endpoint security. According to Intel, there is no clear correlation between performance of security software, as measured by testing organisations[76], and market share.

Results of the market investigation

166. First, according to a substantiated reply of one of McAfee's competitors, the degradation of interoperability would have similar effects as a technical tying of McAfee security software leading to the exclusion of McAfee's competitors from Intel's platform. In essence, these effects would be similar because McAfee security solutions would be the only ones that fully and optimally function with Intel platform's features. It also indicates that such degradation in conjunction with a strong marketing campaign for the new Intel/McAfee combination would result in security software from other vendors being perceived as less effective: "*If Intel denied interoperability with ISVs' software post-transaction, this would in effect amount to technical tying of McAfee security software (and the exclusion of ISVs from the Intel environment).* […] *If Intel were to delay provision of information to ISVs, and/or degrade interoperability with their products (likely in conjunction with a strong marketing campaign), ISVs' security software would ultimately be perceived as less effective, in particular when operating on Intel hardware. Since customers would not accept lower performing security software (given the increase in cyber crime), McAfee's products and solutions would be chosen over those of other ISVs, resulting in significant revenue losses for* [us]."[77]

---

76 See for instance www.av-comparatives.org or www.av-test.org.

77 Non-confidential reply to the Commission's market investigation.

167. Second, according to some of McAfee's competitors, their entire revenue stemming from endpoint security could be impacted, leading to the exit of some SSVs. While the consequences in terms of price remain unclear at this stage, McAfee competitors foresee reduced innovation and choice. According to one of them, "*competitors of McAfee will be forced to drastically reduce price to try to limit the loss in volume, or downsize and refocus on niche markets. In both cases, the revenues that can be invested for R&D will be heavily impacted. McAfee will be shielded from any competition on innovation due to interoperability and will therefore have no incentive to continue investing in innovative products.* […] *If McAfee is the only security vendor with full access to Intel interoperability, it will become the preferred security solution of any Intel customer. As mentioned, competitors would need to consolidate, flee to niche markets or disappear. In any of these scenarios, consumer choice will be heavily impacted."*[78] According to another McAfee competitor, "*innovation would be hampered, as only McAfee would be allowed to interoperate fully with those resources.* […] *McAfee could become the sole provider of enhanced security via hardware. Intel could let other vendors to interoperate at a baseline of performance, but they would not be able to compete in equal technological terms.* […] *We believe it would be very significant, given Intel's dominance of the CPU market. Security vendors obtain their revenues mostly from their Intel-compatible solutions, so the overlap of customers being potentially affected would be very high. Besides, the impact on the risk of monoculture would also be very high.*"[79]

168. Third, two of Intel's competitors indicate that there would also be a negative impact on chipsets and CPU markets. A degradation of McAfee's interoperability with other chipsets or CPUs suppliers would be likely to further increase barriers to entry on markets where Intel is active by locking out other CPU manufacturers.

169. Fourth, the market investigation suggests that Intel's installed base could be impacted through a microcode update. Moreover, according to one McAfee's competitor, "*it is possible to extend capability and add new options to existing and publicly documented instruction sets without breaking backward compatibility.*"[80] In addition, it cannot be excluded that Intel CPUs contain some dormant instructions that could be activated to work with McAfee in a certain manner. The market investigation is however unclear with regard to the time horizon of such changes in interoperability.

170. Fifth, the market investigation confirmed the importance of performance for market success. According to certain respondents, hardware enabled software could run much faster, which, if reserved to McAfee, could have 'earthquake effects' on the market[81].

---

78 Non-confidential reply to the Commission's market investigation.

79 Non-confidential reply to the Commission's market investigation.

80 Non-confidential reply to the Commission's market investigation.

81 At the question of "*how much memory is available within the CPU* […]?" and whether "*this is sufficient to embed a meaningful form of security solutions?*", one competitor answers that "*the memory required to implement hardware acceleration is small. It is not a matter of actually processing or scanning directly in the hardware (which would require a lot of memory), it is more about encryption support. This was confirmed by Mr. Dave De Walt (CEO McAfee), who spoke at the ISMS Forum in Barcelona, Spain on 30th November 2010 about the merger and what it brings to McAfee. He clearly stated that the focus will be on hardware acceleration for encryption. He also stated that the performance will be 50 – 100 times*

171. Sixth, several internal documents from McAfee envisage the hardwiring of security as a game changer that no other competitor would have the possibility to replicate. For instance, in a document of 13 June 2009, the deal is presented as a "*true game changer*" […].

Results of Commission assessment

172. The Commission considers it likely that the effects of an interoperability hampering by Intel will be significant on the endpoint security and CPUs / chipsets markets, in particular with regard to innovation and choice.

2.4. Conclusion

173. The Commission considers it likely that Intel has the ability and incentives to hamper interoperability and that the negative effects of such a practice on the relevant markets would be significant. On the basis of the replies received, the market investigation also provided evidence that such a strategy will give rise to serious doubts as to the compatibility of the transaction with the internal market.

174. The Commission concludes, also in the light of the results of the market investigation, that it is likely that the conglomerate effects resulting from a degradation of the interoperability between the parties' products and those of the parties' competitors would lead to foreclosure of McAfee's competitors in the endpoint security markets and thereby possibly strengthen the current dominant position of Intel in the chipset and CPU markets.

3. Assessment of a foreclosure strategy based on technical tying

175. Technical tying consists in the technical combination of products of both parties in a persistent form, i.e. in the embedding of security solutions in Intel's CPU and chipsets platforms.

176. In order to prevent any foreclosure on the security solutions market stemming from embedding security software in to Intel's hardware, ensuring interoperability between the solutions developed by McAfee competitors and Intel's hardware would not necessarily be sufficient. Indeed, the persistence of embedded software solutions from McAfee's into Intel hardware could interfere with the functioning of alternative security solutions.

3.1. Ability of Intel to technically tie

The notifying party's view

177. First, Intel submits that CPUs are 'software agnostic' (i.e. they cannot discriminate according to the origin of the instructions they receive) and their instructions can be exploited by all software. Therefore, according to Intel, it is not possible to provide instructions that can be used by some software vendors, but not by others.

---

better than a software-only solution. If this technology will be only available for McAfee, the other vendors will never be able to compete – the advantage of McAfee's solution will be huge."

178. Second, according to Intel, a number of third-parties play an important role in how Intel hardware interacts with software applications. In particular, OEMs or vendors of OS or BIOS would be able to prevent Intel from controlling the (de-) activation of certain CPU features.

179. Third, Intel argues that there are a number of technical constraints that would prevent Intel from embedding software into hardware, notably the limited space available within a CPU and the necessary updating of software.

180. In order to support these arguments, Intel has submitted two reports from IT experts[82].

Results of the market investigation

181. Respondents to the market investigation generally consider that Intel has the ability to technically bundle its hardware components with certain features of the security solutions developed by McAfee. They refer in particular to the feasibility of the following strategies.

182. First, embedding of at least basic McAfee antivirus protection in all mainstream Intel CPU and chipsets platforms would be feasible. This would make some of the equivalent features of competing security solutions redundant and possibly also less efficient if the embedded McAfee solution interferes with the effective running of competing security solutions. Many refer to Intel's existing vPro suite of technologies[83], which already today contains some security functions at the chipset level, and which could be significantly further enhanced with McAfee's security solutions. Elements of vPro (including the virtualization technology at the CPU level) could therefore be a starting point for this strategy.

183. Second, certain security tools (notably encryption) which are currently performed in software could be embedded in hardware at the CPU level. In addition to embedding these security solutions into Intel's hardware, Intel could reserve instructions and interfaces that are needed for the embedded solution to McAfee by keeping them secret.

184. Third, Intel could use the vPro components (notably AMT and TXT) - and the remote manageability which these components allow - to embed a McAfee antimalware agent in Intel hardware which could then be activated, operated and monetised through a McAfee cloud infrastructure with updated malware databases in the cloud.

185. Fourth, Intel could insert a non-wipeable hidden sleeper agent within the CPU/Chipset/peripheral which can be activated and monetised after the purchase of

---

82 Report on the Implications for Microprocessor Design following an Intel-McAfee Merger by Dr. Gregory Papadopoulos and Expert report of Mr. Nathan A. Brookwood.

83 Intel vPro is a combination of processor technologies, hardware enhancements, management features, and security technologies including software that allow for example remote access to the PC (including monitoring, maintenance, and management) independently of the state of the OS or power state of the PC. It comprises different technologies such as hardware assisted virtualisation under the VT brand, a trusted execution environment under the TXT brand and a remote management technology under the AMT brand. All those technologies are marketed by Intel together under the vPro brand and sold bundled together with Intel CPUs and chipsets.

computing device to allow remote controlled operations in favour of McAfee software. One McAfee's competitor indicates that by doing so Intel could replicate in the security field what it has recently implemented for its Pentium CPU[84], i.e. deliver embedded McAfee software as a hidden upfront bundle and "unlock" the solution only at a later stage.

186. Fifth, soft bundling tactics through promotional pop ups on the screen are also considered as technically feasible. However the market investigation shows that for commercial reasons this could be difficult to implement since such popups would require the support of the OS.

187. Sixth, the market investigation suggests that the implementation of soft bundling tactics to make preinstalled McAfee software more persistent and second sales difficult or impossible is technologically feasible.

188. The majority of respondents also considers that given Intel's dominant position and today's commercial reality, if Intel wanted to implement such strategies, other players such as OEMs and BIOS vendors would not be able or have the incentives to prevent Intel from doing so.

189. In order to demonstrate that the scenarios above are likely and not just speculative, one respondent to the market investigation refers to the fact that Intel has filed extensive patent applications in the US, including an application relating to a method, apparatus and system to enable a secure location-aware platform: "*Specifically, embodiments of the present invention may utilize a secure processing partition on the platform to determine a location of the platform and dynamically apply and/or change security controls accordingly.* […] The application states that "*…the ability to apply more stringent and better security controls based on the trustworthiness of the network is typically left to security vendors. Most vendors do not, however, provide configurable controls based on system location.*"[85] While the access to interoperability information would be a condition to enable SSVs to provide configurable controls based on system location, it would not be sufficient because SSVs would also need to be in a position to disable such features if they are not compatible with the security solutions elaborated by them.

190. Intel's claim according to which CPUs are software agnostic is confirmed only as regards the CPU in a narrow sense and only as regards the situation today. However, the market investigation suggests that this situation could evolve under different incentives and that there are no technical constraints that would hamper such an evolution. According to an independent respondent to the market investigation, "*modern processors have many performance features that can only be exploited by software that is aware of a given feature, and in that sense all modern processors are not software agnostic. Modern processors can already indirectly determine the software that is issuing (originating) a given set of instructions.* […] *It is possible for a complex CPU to incorporate an explicit registration mechanism for one software application to uniquely*

---

84 According to this respondent, the latter model is already being tested in relation to certain of its chips, whereby Pentium chips that are better than advertised are included in some low-end desktop computers. Customers subsequently pay an additional fee to "unlock" their full power.

85 Abstract from Patent Application US 20080092236 A1, available at: http://www.freepatentsonline.com/20080092236.pdf.

identify and unlock special/hidden capabilities for that given software application that would not be available to other competing, equally capable software applications. However, [we have] *no knowledge of this specific situation involving Intel and McAfee.*"[86] It is worth noting that even if such an explicit registration mechanism was designed so as to run non exclusively with a McAfee solution, the persistence of the McAfee solution embedded into Intel's hardware might preclude or interfere with the effective running of competing security solutions.

191. Moreover, the claim that Intel's products are software agnostic is largely dismissed for peripheral hardware components such as the vPro technologies. In particular, several respondents to the market investigation point to Intel's existing AMT technology that would enable the locking down of certain functions to specific software. A third party IT expert indicates that "*Intel AMT is a great example of how Intel can reserve/lock down some functionality only for its own software. Intel AMT software is being kept on a flash chip on the motherboard (might not be produced by Intel), but the Intel chipset (which has recently been integrated onto the processor die, in Intel Core i5/i7 processors) verifies if the AMT code is signed with Intel digital certificate, and only then allows execution of this code on the chipset's internal processor (the "AMT processor"). The "AMT processor" is a small processor located in the chipset (more specifically in the north bridge), that has privileged access (i.e. beyond OS control) to certain system resources, such as memory and network cards. Intel AMT allows for creating powerful system management solutions that can be used even in case the OS on the target computer is malfunctioning, and thus allow for powerful remote recovery.*"[87]

192. Similarly, Intel's argument on the limited memory available at the CPU level is infirmed by the market investigation, and some respondents to the market investigation also indicate that in any event other technology components at the chipset level could be used with comparable effects. According to one McAfee's competitor, "*recent developments in Intel's products, including the introduction of its vPro technologies and the broader use of virtualisation technologies, mean that memory constraints impose no material restrictions on Intel embedding security software in the silicon."*[88]

193. According to another McAfee competitor, "*the memory required to implement hardware acceleration is small. It is not a matter of actually processing or scanning directly in the hardware (which would require a lot of memory), it is more about encryption support. This was confirmed by Dave De Walt (CEO McAfee), who spoke at the ISMS Forum in Barcelona, Spain on 30th November 2010 about the merger and what it brings to McAfee. He clearly stated that the focus will be on hardware acceleration for encryption. He also stated that the performance will be 50 – 100 times better than a software-only solution.*"[89]

194. Finally, as mentioned above and contrary to what Intel claims, the market investigation suggests that the BIOS vendors, OS developers, OEMs and users have in

---

86 Non-confidential reply to the Commission's market investigation.

87 Non-confidential reply to the Commission's market investigation.

88 Non-confidential reply to the Commission's market investigation.

89 Non-confidential reply to the Commission's market investigation.

today's commercial reality no real ability to intercept and unbundle such solutions. According to one OEM, "*OEMs and users will be restricted in their free selection of security SW; Bios and OS vendors have no incentives to defeat.*"[90]

195. Moreover, according to one Intel competitor: "[We] *believe* […] *this depends on what Intel's design permits. Locked hardware structures may be impossible for BIOS vendors, OEMs or OS vendors to unlock and are probably impossible for most users to unlock.*"[91]

196. The conclusion that Intel can embed endpoint security solutions in its CPU and chipset platforms is also supported by […][documents from the parties].[92]

197. Finally, a number of statements of Intel's executives tend to confirm Intel's ability to embed endpoint security solutions in its hardware. Intel CEO Paul Otellini noted in various articles and on 19 August 2010 at a press conference, that "[Intel] *believe*[s] *security is most effective when enabled in hardware.*"[93] During the same press conference, he added that "*Joining the assets of McAfee with Intel will accelerate and enhance the combination of hardware and software solutions.*"[94] He added also that " *we began to understand* […] *that having a deeper collaboration, where we could look long term and try to look at the combination, the deeply-integrated combination of hardware and software capabilities, would add substantial value to our platforms and differentiation to our platforms, number one.*"[95] Intel Senior Vice President Renée James said the same day that "*the proposed acquisition of McAfee executes against Intel's software strategy to grow our business by using software to enhance hardware. We've done this successfully with over a dozen software acquisitions, including Wind River and Havok, which represents a fundamental belief that the most pressing problems in computing will require both hardware and software solutions.* […] *We also recently launched the Intel anti-theft technology, which will disable a computer if it's lost or stolen. Our teams have been working together to build enhanced security solutions that can better protect consumers and the industry from malicious events. Through this partnership we've had an opportunity to learn about McAfee, the possibilities of what a closer partnership between hardware and software could bring.* […] *We believe we can have products in the market, these enhanced products in the market, in the first part of 2011* […]. *The underlying hardware technology ships in our core products today and will be extended into Atom in the near future. So these are already existing hardware features and functionality that can enhance security software like the products from McAfee, in addition to the cloud services that McAfee offers. So there's some amount of work that has to be undertaken between the two of us that has been going on, as we said,*

---

90 Non-confidential reply to the Commission's market investigation.

91 Non-confidential reply to the Commission's market investigation.

92 […].

93 http://www.faqs.org/sec-filings/100819/INTEL-CORP_8-K_FORM2/dex991.htm.

94 http://www.faqs.org/sec-filings/100819/INTEL-CORP_8-K_FORM2/dex991.htm.

95 http://www.faqs.org/sec-filings/100819/INTEL-CORP_8-K_FORM2/dex991.htm.

for the last about 18 months. So we don't need to come out with brand-new silicon, we have the underlying features available now". [96]

Results of the Commission assessment

198. The replies to the market investigation received, a number of internal documents of the parties, as well as public statements from Mr. Otellini and Ms. James suggest that Intel can technically tie its chipsets / CPUs with McAfee's endpoint solutions. The Commission concludes therefore that it is likely that Intel has the ability to engage in technical tying.

3.2. Incentives of Intel to technically tie

The notifying party's view

199. According to Intel, it has no incentive to engage in technical tying because it needs broad based software support. According to the notifying party, one of the driving factors behind McAfee's ePO[97] and Intel's hardware success in the enterprise segment is the open nature of their platforms. Engaging in technical tying would damage Intel's relationship with partners on whom it depends. Intel's partners are unlikely to lend their support to costly changes to computers that would only benefit Intel/McAfee.

200. Moreover, a technical tie would threaten the broad based software support on which Intel relies to drive demand for its processors with enterprise customers. According to the notifying party, these customers are sophisticated buyers that value flexibility and are knowledgeable about substitutes. Any attempt to impose a technological tie would put at risk both microprocessor and security software sales.

201. Furthermore, Intel claims that it is not able to persuade OEMs to adopt Intel solutions that do not bring clear significant end user benefits and, on this account, it refers to two recent examples, namely the Viiv platform and the Itanium processor the introduction of which failed because of the lack of support from OEMs.

202. Lastly, according to Intel, there is an important distinction to be made between technical tying (which is making inseparable products that can equally function separately) and product integration (which is integrating products to improve their global performance). According to Intel, while it has never engaged in technological tying, it has integrated new functionalities into its microprocessors and chipsets, whereby bringing substantial improvements in terms of performance, functionality or reduction of costs for its customers. Intel refers to several examples of such product integration that occurred on its platforms as well as competing platforms[98]. In other words, according to Intel, the migration of certain features into Intel's hardware has never been a mere

---

96 http://www.faqs.org/sec-filings/100819/INTEL-CORP_8-K_FORM2/dex991.htm.

97 ePO is an enterprise management console which is open and compatible with software by McAfee's competitors.

98 Examples quoted by the Intel are: the migration of a math co-processor, of the level 2 cache memory component, of the memory controller into the microprocessor, the migration of the graphics controller onto the chipset and recently into the microprocessor core, the integration of separate microprocessors cores on a single microprocessor chip, the integration of the power supply transistor control onto the processor die.

combination of separated products but has always resulted in global product enhancement.

Results of the market investigation

203. The market investigation refers to several examples of technical tying/bundling in Intel's history including the following: (i) combination of Intel's CPU with wireless technologies that were previously implemented in separate semiconductor products, (ii) chipsets including Macrovision copy protection technology, without a real necessity for the final product, (iii) integration of graphics in the CPU die.

204. According to one of Intel's competitors, Intel has also successfully bundled hardware and firmware features to create their vPro brand creating a premium tier for which they are the sole provider and despite the existence of competitive solutions for most technical capabilities and the fact that many features go unused in most customers' environment. It says that "*Intel has successfully bundled hardware and firmware features to create their vPro brand offering, a product with higher prices and margins. vPro is an Intel brand representing a number of technologies and capabilities, some of which are also available under separate brands, and sometimes no Intel brand. Intel worked directly with IT departments at many large and small enterprises to create a demand for vPro branded PCs, while also offering incentives for OEMs to provide PCs under this vPro brand. Despite the fact that there are competitive solutions for most of the technical capabilities that fall under the vPro brand umbrella, or that many of the vPro branded features go unused in customer environments, Intel successfully created a premium tier for which they are the sole provider given its significant market share in the CPU market.*"[99]

205. According to one OEM, incentives of Intel might include product innovation, elimination of double marginalisation allowing it to lower prices to OEMs, which would both be positive evolutions, but might also include a desire to reduce competition in the complementary product, or to reduce competition in CPUs by reducing innovation and viability of products that could be used with competing CPUs.[100]

206. The market investigation also suggests that it is unlikely that Intel could lose CPU sales from a technical tying strategy given the "must-stock" status of Intel's hardware. According to one McAfee's competitor, "*since security software will always be required, linking it to Intel's "must-stock" hardware (with associated marketing suggesting a "safer" CPU) will create a "virtuous circle" of demand. Against this background there would be no reason for OEMs to object to the technical tying of security software with Intel hardware. Even if they did, they could only attempt to switch a very marginal percentage of their CPU requirements (to CPUs without any security software) given Intel's established "must-stock" status and the fact that AMD has not yet developed the equivalent of Intel's vPro technologies.*"[101] Two respondents to the market investigation

---

99 Non-confidential reply to the Commission's market investigation.

100 Non-confidential reply to the Commission's market investigation.

101 Non-confidential reply to the Commission's market investigation.

make a link between this question and interoperability. One OEM considers that if the implementation does not negatively impact other security solutions, it is not to expect that it negatively impacts Intel CPU business. According to one customer, a loss of CPU sales could happen, if customers do not want to use McAfee's product.

207. Moreover, several respondents to the market investigation doubt that antitrust rules constitute an effective deterrent in relation to technical tying. According to one of them, Intel's repeated infringements of antitrust rules in the past together with its reactions denying the findings of the regulatory authorities are an indication that antitrust reaction would no act as a deterrent to Intel. Perhaps most importantly, some respondents to the market investigation claim that previous cases such as the Microsoft case show that antitrust enforcement usually comes too late to restore competition.

208. The market investigation suggests that Intel competitors could perhaps try to create a competing solution. However, some respondents to the market investigation doubt that such a counter-strategy, in light of the limited market share of the competitors and the time necessary to go to the market, would be successful.

209. The possibility of an effective counterstrategy by OEMs is also regarded as doubtful given Intel's market power.

210. During its investigation, the Commission assessed several internal documents of the parties. According to one document, the embedding of security into silicon would be a "*True game changer – […]*.[102] Other internal documents point into the same direction.[103]

Results of Commission assessment

211. Taking into account the above, the Commission concludes that it is likely that Intel has incentives to engage in technical tying.

3.3 Effects on markets

The notifying party's view

212. According to Intel, even if it could engage in technical tying and had the incentive to do so, this would not result in substantial foreclosure. For instance, even if Intel were able either to integrate McAfee software into Intel silicon or promote McAfee software through an advertising “stub”, this would not foreclose any McAfee competitor. These steps might reduce McAfee’s distribution or promotional costs, but McAfee competitors would remain able to compete with the same access to Intel microprocessor functionality as they have today.

---

[102] […].

[103] […].

Results of the market investigation

213. As regards the impact on the security software market, some respondents to the market investigation expect a significant impact with the exit of certain software developers. Indeed, two respondents indicate that Intel competitors like AMD would not enable SSVs to reach a critical mass to compete with Intel/McAfee. Because Intel/McAfee would be the sole provider of hardware enhanced security, competitors would not be able to compete on equal technological terms. According to one respondent, ISVs would effectively be forced into the position of having to make a second sale to compete with the technically tied offering. Even though, this would not be tenable because, on the one hand, the security component embedded into the hardware would be extremely difficult to uninstall and, on the other hand, running multiple versions of security software would not be practicable, resulting in unacceptable performance, increased risk of system instability and no real improvement in security.

214. A number of respondents consider that ultimately choice will be reduced and prices of security software will be driven down which will reduce available funding for R&D. According to one respondent, "*the rest of the security industry would compete for the remaining available market space. This would leave security vendors to increase prices to be able to fund innovation on specialised markets. Alternatively, and more realistically they would lower the price, which would result in companies not being able to invest in people and innovation. In that process, some vendors may be driven out of the market limiting choice for customers and reducing innovation.*"[104] On the other hand, two respondents indicate that innovation could be fostered by such a strategy.

215. Moreover, with regard to efficiencies, while some respondents to the market investigation do not exclude them, the market investigation suggests that any efficiencies resulting from technical tying should be balanced against the risk of a security software "monoculture" with a "single point of failure" stemming from such a strategy. According to one respondent of the market investigation, *"the efficiency in collaborating more closely with a particular security vendor excludes competition from the market. This leads to dependence on a particular security solution. Whilst this may be a technically superior product it will nevertheless be targeted by hackers meaning that it actually is less secure than it would have been in a market with a diverse number of products where hackers' efforts were less targeted. The efficiencies themselves intrinsically cause consumer harm".*[105]

216. According to one McAfee competitor, "*the general content security business relies heavily on the diversity of its offerings. A monoculture approach would lead to a single attack target as we've experienced in the past 15 years with Microsoft products, regardless of how safe they've been made. With Intel dominating the CPU and Chipset market at 84% we are on the edge of a similar risk. If they are allowed to bring in their*

[104] Non-confidential reply to the Commission's market investigation.

[105] Non-confidential reply to the Commission's market investigation.

ower to dominate the security solutions it will be just a question of time before attacks are focused on this single solution."[106]

217. Finally, the market investigation suggests that technical tying might lead to a significant increase of Intel's market share and/or the prices on the computer CPU markets. One respondent to the market investigation considers in particular that Intel/McAfee will have a *de facto* monopoly and could charge high prices for its hardware offering security features; moreover, once the products are launched, Intel will have reduced incentive to further invest in R&D. According to another respondent to the market investigation, the impact could be notably significant in the corporate segment/market. However, none of these concerns were substantiated. Moreover, some respondents to the market investigation anticipate an impact on other types of CPUs, such as handheld, embedded devices and consumer electronics.

Results of Commission assessment

218. In the light of the above, the Commission considers that the possible foreclosure of SSVs stemming from a possible technical tying and the resulting lack of access to Intel hardware or interference of tied McAfee solutions with competitors' products, gives rise to serious doubts as to the compatibility of the proposed transaction with the internal market.

3.4 Conclusion

219. The Commission considers it likely that Intel has the ability and incentives to technically tie its products with McAfee's endpoint security and that the negative effects of such a practice on the relevant markets would be significant.

220. On the basis of the replies received, the market investigation also provides evidence that such a strategy would give rise to serious doubts as to the compatibility of the transaction with the internal market.

221. The Commission concludes, also in the light of the results of the market investigation, that it is likely that the conglomerate effects resulting from a technical tie between the parties' products would lead to the foreclosure of McAfee's competitors in the endpoint security markets and thereby possibly to the strengthening of the current dominant position of Intel in the chipset and CPU markets.

4. Assessment of a foreclosure strategy based on commercial bundling

222. The Commission has assessed the likelihood of two forms of commercial bundling: pure and mixed bundling.

223. In the present case, pure bundling would imply that CPUs and security software are sold exclusively together while mixed bundling would imply that either the CPUs or the security software would be offered at a discount when customers buy both products from Intel/McAfee.

---

[106] Non-confidential reply to the Commission's market investigation.

4.1. Ability of Intel to commercially bundle

The notifying party's view

224. According to Intel, the merged entity would not have the ability to implement a commercial bundling strategy, either under a pure or mixed form. In its submissions, Intel has not made the distinction between the two types of commercial bundling.

225. First, Intel gives past examples (Viiv and Itanium) allegedly demonstrating that it does not have the ability to impose the adoption of hardware or software technologies on OEMs. According to Intel, where user benefits were not clear and significant, OEMs have been in a position to refuse to incorporate these technologies.

226. Second, Intel claims that OEMs enjoy substantial countervailing buyer power and it would therefore have limited ability to impose its products to them. According to Intel, there is significant competition between CPU vendors to convince OEMs to adopt their products. OEMs take into account a number of factors relating to the CPU, such as price, performance, reliability, consistency, strength of technological solutions or platforms, strength of 'roadmaps' of future product offerings, supply capacity, technical and marketing support, and brand. OEMs typically seek a single CPU supplier to supply their entire requirements for each model. According to Intel, a second point at which OEMs can exercise leverage is when buying CPUs for installation in their PCs, since a design win does not entail a commitment by the OEM to sell a particular number of systems based on the new platform. This would mean that CPUs suppliers are facing constant rounds of competition.

227. Third, Intel claims that OEMs also have significant leverage in negotiating for security software. OEMs regularly invite SSVs to participate in competitive bidding contests. They generally expect the winning vendors to make upfront payments in return for the pre-installation of their software and/or to share sales revenue when consumers start paying for the software after expiry of the free trial period. According to Intel, the transaction will not enable Intel to significantly reduce these 'bounty costs' as it feels that OEMs would not accept to have lower revenues from pre-installation.

228. Finally, Intel argues that commercial bundling is not possible because CPUs and security solutions have different contract cycles and parameters of negotiation, and customers should consequently not be considered as a common pool. In the EC non-horizontal mergers guidelines, a common pool of customers is one of the factors regarded as necessary to establish the ability to foreclose.[107]

229. Intel would therefore encounter practical difficulties to enter into a commercial bundling strategy. According to Intel, sales of CPUs for consumer PCs are typically negotiated on a quarterly basis while security software contracts typically cover multiple

---

[107] See paragraph 100: "[…] *for foreclosure to be a potential concern, it must be the case that there is a large common pool of customers for the individual products concerned. The more customers tend to buy both products (instead of only one of the products), the more demand for the individual products may be affected through bundling or tying. Such a correspondence in purchasing behaviour is more likely to be significant when the products in question are complementary.*"

years and the pricing terms for security software are complex. While there is some upfront payment by the SSVs, there is also typically a risk-sharing provision that is based on conversion and renewal rates.

230. Given all the variables associated with security software, attempting to commercially bundle the products together would be difficult for Intel.

Results of the market investigation

231. The market investigation confirms that Intel possesses strong seller power. This is reflected in particular (i) by Intel's market share in CPUs sourcing which fluctuates between [70%-80%] and [90%-100%] and (ii) the must-stock nature of Intel's brand. AMD appears nowadays as a lower price, but also weaker alternative even if certain OEMs consider that they are able to switch a certain part of their requirements from Intel to AMD.

232. The market investigation suggests that Intel would therefore have the ability to promote a commercial bundle, for example through exclusionary mixed rebates between Intel's CPUs and McAfee's endpoint security. Given Intel's dominant position in the chipset/CPU markets, Intel could use such exclusionary conditional rebates to push McAfee's products onto OEMs.

233. Conversely only few OEMs claim that they possess countervailing buyer power vis-à-vis Intel. According to one of them, "*like other OEMs*, [it] *has an ability to negotiate and maintain an appropriate buy / sell relationship with Intel*"[108]. There are only two out of seven OEMs considering that they are key customers for Intel. A majority of OEMs and more generally Intel's customers are however of the opinion that Intel is a must-have partner with whom it is difficult to negotiate.

234. As regards Intel's alleged limited ability to commercially bundle in the absence of a significant common pool of customers, most OEMs confirm that there would be some practical difficulties with such a strategy. Contract cycles and durations for CPUs and security solutions are currently different. Negotiations are currently also often led by different teams for each of these products.

235. However, according to some of McAfee's competitors, negotiation and contract formats can be changed in particular if a company with market power such as Intel requests to do so.

236. Two OEMs indicate that they could consider preloading McAfee security software for the next contract negotiations if Intel requested it. Three other OEMs do not.

Results of Commission assessment

237. It seems likely that following the proposed transaction Intel may be able to change commercial patterns. The investigation has clearly confirmed Intel's bargaining power towards OEM, with limited possibilities for the later to react. In addition, Intel internal documents dating before the proposed transaction show that one of the reasons why Intel

108 Non-confidential reply to the Commission's market investigation.

chose to acquire McAfee and not other smaller vendors was the synergy potential given the relationships with major OEMs.

238. The Commission considers therefore that it is likely that Intel has the ability to enter into a foreclosure strategy through a commercial bundling between its chipsets / CPUs and McAfee's endpoint security.

4.2. Incentives of Intel to commercially bundle

The notifying party's view

239. Intel claims that it has no economic incentive to bundle the sale of McAfee's software solutions to the sale of its chipsets / CPUs.

240. First, the increase in market share would be limited. A commercial bundling would affect only the McAfee revenues obtained through the OEM channel. As mentioned in paragraph 88, the OEM channel only represents […]% of McAfee's revenue in the consumer segment (that represents itself […]% of McAfee's total revenue). The OEM channel represents therefore around […]% of the total McAfee's revenues.

241. Intel claims that, on the contrary, it has every interest in protecting its CPUs sales revenue (currently around USD […] million) by making sure that these CPUs remain compatible with the broadest range of software products, including those of all SSVs. Intel claims that it would no doubt lose market share to AMD if it tied the sales of its chipsets / CPUs to that of McAfee's endpoint security.

242. Alternatively, Intel considers that any hypothetical bundle for a package consisting of chipsets / CPUs and an advertising agreement for endpoint security software would potentially increase the payments to OEMs for the right to have McAfee software distributed with the OEMs' PCs, rather than a decrease in the payment to the OEM. This claim is confirmed by certain Intel internal documents[109].

243. Intel also claims that its past practices demonstrate that from its point of view it has not engaged in pure bundling or tying previously, although it has offered bundled discounts in a number of cases.

244. With regard to previously bundled sales of chipsets and CPUs, Intel argues that the transactions typically originated with requests from OEM customers for Intel to meet competition based on price quotes on competitors' CPUs and chipsets. This would have stemmed from the fact that because chipsets for Intel and AMD CPUs are not interchangeable, the combined price of the two components was most relevant to an OEM that is comparing the cost of using an Intel CPU versus an AMD CPU.

245. With regard to Centrino mobile technology, from 2003 to 2009, Intel claims that it offered discounts to OEMs in connection with its Centrino mobile technology ("CMT"), which consisted of a CPU, a chipset, and a wireless ("Wi-Fi") connection. The principal purpose of these discounts was to promote the adoption of a new usage model focused on mobility which was new at that time.

---

[109] […].

246. With regard to the Atom CPU, Intel claims that it offered a bundled price for its Atom CPU and companion chipset according to Intel merely as a convenience to OEMs. Intel offered a discounted price for the CPU alone for OEMs that wished to buy only the CPU.

247. Intel claims that all these previous commercial bundling practices were not anti-competitive.

248. Intel also describes past examples where it decided not to bundle, whereas it would have been easy to do so. This would have been the case for motherboards and solid state drives ("SSDs") that Intel also manufactures.

249. Intel has also retained external economic advisors[110] who have submitted a quantification of a "*Foreclosure and Critical Loss Calculation*" which attempts to quantify Intel's future incentives and economic effects of certain hypothetical business practices. The submission focuses on the hypothetical scenario in which Intel commercially bundles its hardware to McAfee software and aims to demonstrate the effects of this conduct in the OEM distribution channel.

250. It concludes that any commercial bundling strategy would be unprofitable: according to the studies provided, the maximum market share gain for McAfee that could be achieved through a bundling strategy would be [less than 1%]. Moreover, a mere loss of [less than 1%] of Intel's CPU sales would make such a strategy unprofitable.

251. Intel claims that it could not take any such risk since its capacity utilization is critical to its profitability. One of Intel's major competitive advantages is that it manufactures CPUs in-house. CPU manufacturing is largely a fixed cost business, and it is very important for Intel to achieve a high level of capacity utilization. Because Intel's most significant costs are in manufacturing and R&D, margins on incremental sales are high. That would mean that any loss of CPU sales would cause Intel to lose highly profitable incremental sales. Intel enjoys relatively high margins on CPUs because a very large percentage of the cost of its CPUs is fixed. Given that Intel maximizes profits by operating its factories at high levels of capacity utilization, Intel needs to maintain demand at a level high enough to sustain this high-efficiency production. Thus, any strategy that risks the loss of CPU sales would be unattractive to Intel.

Results of the market investigation

252. Contrary to Intel's claims, many respondents to the market investigation indicate that Intel could have incentives to commercially bundle its CPUs with McAfee's security solutions[111]. For instance, according to one McAfee competitor, "*the incentive of bundling the McAfee products together with Intel chips would be the revenues expected from the subscription renewals once the free period expires. In this regard, there is possibly a complete overlap of customers, since computer manufacturers buying Intel*

110 Professor Tim Bresnahan of Stanford, as well as the Economic Consultancies Nera and CornerStone.

111 10 out of 11 respondents to this question.

chips also enter regularly into OEM, pre-installation agreements with anti-malware vendors." [112]

253. Although the respondents to the market investigation do not all refer to specific past examples of Intel mixed bundling, some of them provide evidence of such practices. The bundled sales of Intel Centrino mobile technology, of Intel vPro technology, of Intel chipsets as well as of Intel GPUs are four examples of commercial bundling frequently mentioned by complainants (see paragraph 204).

254. Moreover, some respondents to the market investigation that have referred to Intel's bundling of its Centrino brand do not consider this as a pro-competitive practice. Until January 2010, this brand covered a particular combination of mainboard chipset, mobile CPU and Wi-Fi connection in the design of a laptop. Intel claimed systems equipped with these technologies deliver better performance, longer battery life and broad wireless network interoperability. Despite resistance of OEMs that considered that the bundle was underperforming, according to some respondents to the market investigation, Intel sold this commercial bundle from 2003 to 2010. While this example refers to the bundling of hardware components and not to the bundling of hardware and software, it is illustrative of Intel's power vis-à-vis the OEMs, of Intel's past practices and of Intel's incentive to bundling together products of different quality and interest.

255. In the present case, the market investigation suggests that through mixed bundling practices Intel would be able to significantly strengthen its market power in the endpoint security market and might even reinforce its position in the CPU markets.

256. Moreover, the majority of the respondents to the market investigation does not think that such a strategy would lead to a material loss of CPU revenues for Intel. According to one McAfee's competitor, "*if there is any loss of CPU sales at all, this will be vastly compensated by increased software revenues and brand penetration.*"[113] Another McAfee's competitor indicates that "*the use of mixed rebates would enable Intel to take advantage of the hundreds of dollars per PC that flow between it and the OEMs (relating to sales of CPUs, chipsets and/or entire motherboards to OEMs and rebates, market development funds and other dollars that flow back from Intel to the OEMs) to win McAfee placement on OEM systems*".[114]

257. The market investigation is mixed as regards the possible counter-strategies which could be adopted in case of commercial bundling.

258. Customers generally do not object to Intel following such a strategy since they would benefit from a price decrease. They also say that commercially it would be difficult for them to switch to another CPU provider if they want to resist the bundling strategy.

259. Some of McAfee's competitors state that they would either have to exit the market or try to reach an agreement with AMD, which would however have much less leverage than Intel. For instance, one of them explains that it is "*open to engage in conversations*

---

[112] Non-confidential reply to the Commission's market investigation.

[113] Non-confidential reply to the Commission's market investigation.

[114] Non-confidential reply to the Commission's market investigation.

with other CPU manufacturers, even if [it] *believe*[s] *the potential effect would be limited.*"[115]

260. Some other competitors exclude this later option. For instance, one of them considers that it would not be able to cooperate with another CPU manufacturer: "[we] *do* […] *not believe any cooperation with another CPU manufacturer would be capable of replicating the bargaining position Intel has with OEMs.*"[116].

261. One of Intel's competitors considers that it would be very difficult for it to counter such a strategy since it does not have the resources of Intel nor the market position and it would be placed at a significant time to market disadvantage.

262. A majority of the respondents to the market investigation considers however that antitrust rules and enforcement might act to a certain degree as deterrent for anticompetitive mixed bundling.[117] This might be explained by the fact that (i) such practices are relatively easy to detect by antitrust enforcers and (ii) in recent years Intel has been subject to antitrust enforcement against exclusionary rebates and commercial bundling tactics in several jurisdictions. Intel has also settled several cases and promised not to engage in similar practices any longer.

263. On the other hand, a few respondents to the market investigation indicate that preventing a possible antitrust infringement through mixed rebates is difficult and takes so much time that it might come too late. One McAfee competitor explains that "*provided that* [it] *is in a position to detect the infringement and collect sufficiently credible information,* [it] *would contact anti-trust authorities. However, because of the time that this takes, by the time* [it] *has been able to make a case credible enough to bring an anti-trust authority to open an investigation, Intel may already have been successful in altering the structure of competition in the security solutions market*".[118]

Results of Commission assessment

264. Responses to the market investigation as well as past commercial bundling practices suggest that Intel might have incentives to commercially bundle hardware and security software products.

265. On the other hand, a majority of respondents to the market investigation consider that antitrust enforcement may act to a certain extent as an effective deterrent against exclusionary commercial bundling practices.

266. The economic analysis submitted by Intel, as explained above, raises two further important points.

267. First, it claims that the share of sales of all endpoint security software which could be shifted to McAfee by a tying or bundling strategy is low [less than 1%].

---

115 Non-confidential reply to the Commission's market investigation.

116 Non-confidential reply to the Commission's market investigation.

117 8 out of 12 respondents to this question.

118 Non-confidential reply to the Commission's market investigation.

268. The share of endpoint security software sales which could be potentially foreclosed by bundling in the OEM segment is calculated as follows. The consumer segment is estimated to represent [40-50]% of the PC market. [80-90]% of these PC are equipped with Intel processor. Approximately [60-70]% of consumer PCs ship with security software trials, of which [40-50]% are estimated to be provided by McAfee competitors. Multiplying these numbers yields that approximately ([5-10]%) of new consumer and enterprise PCs can be affected by bundling which would shift preloaded security software trials to McAfee. An estimated [0-5]% of these trials actually result in a security software subscription.[119] Taking into account that only approximately [90-100]% of PCs are protected and some software sales are due to subscription renewals rather than new subscriptions[120], the share of sales of all endpoint security solutions that could be shifted by bundling in a given year is [less than 1%].

269. Second, it provides a calculation for the critical loss accrued by Intel which would render commercial bundling unprofitable. The critical loss is defined as "*the share of lost hardware sales that would result in a loss of profit to the merged firm that exactly offsets the profit gained by it from incremental* [*security software*] *trials.*[121]" The submission claims that commercial bundling would be unprofitable if [less than 1%] of Intel's hardware sales were switched away from Intel.

270. The critical loss on Intel hardware which would render bundling unprofitable is calculated as follows. Given that Intel's average profit on hardware (CPUs and chipsets) is approximately USD […] per PC and McAfee's expected lifetime profit on an incremental trial is USD […], Intel would win USD […] on every PC with an additional McAfee trial, but would lose USD […] on each computer for which the OEM switches away from Intel instead of accepting the bundle. This corresponds to a ratio of gains to losses of [0-5]% on every affected PC.[122] Taken into account the share of consumer PC shipments affected ([5-10]%) and Intel's share on these, bundling would be unprofitable if [less than 1%] of Intel's hardware sales were switched away from Intel.

271. The submission claims that Intel had no incentive to foreclose the OEM channel because this channel accounts for a small share of endpoint security software licenses overall. It claims that the OEM channel is primarily an advertising channel: since sales realized through the OEM channel correspond to only those estimated [0-5]% of consumers who convert their security software trial into a paid subscription, the submission implies that the OEM channel accounts for the sale of very few software licenses.

272. However, for SSVs present in the OEM channel, the picture that emerges from other documents available to the Commission seems to be that this channel is responsible for a

---

119 McAfee's conversion rate of [0-5]% is used as an estimate of the conversion rate realized by other SSVs in the OEM channel. The conversion rate is the share of security software trials which results in a subscription.

120 It is estimated that on average, over the lifetime of a PC (five years), […] initial subscriptions result in […] security software subscription payments per year. (see […], footnote 38).

121 […].

122 […].

significant share of the revenues. In particular, based on the information provided by the parties, it can be estimated that the OEM channel accounts for approximately [10-20]% of the average annual revenues of a SSVs present in this channel.[123] Assuming that approximately [80-90]% of the PCs sold in the OEM channel are equipped with Intel hardware (CPU and chipset), on the long run around [10-20]% ([80-90]% of [10-20]%) of the annual revenues of SSVs present in the OEM channel could be affected by Intel possibly foreclosing the OEM channel.[124] By contrast, it is important to note that this would not affect revenues of SSVs absent from the OEM channel.

273. The Commission reviewed the submitted critical loss calculation and responded to it on 14 December 2010.

274. The Commission in its analysis has used a similar framework as the notifying party has and has maintained a number of the assumptions of Intel. The response of the Commission addressed in particular the question on how much of the sales through the OEM channel would Intel have to lose in order to render its strategy of bundling security software and hardware unprofitable, while the question that the notifying party has asked in its submission is on how much of total sales through all the sales channels would Intel have to lose in order to render such strategy unprofitable.

275. The main argument for such an approach in the response of the Commission was that consumers who can be affected by Intel foreclosing the OEM channel are those, who, within the OEM channel, in the absence of foreclosure would purchase Intel hardware with a non-McAfee antivirus preinstalled. Some of the affected customers who wanted to refuse the bundle would switch to an AMD solution within the OEM channel and some would switch to a non-OEM channel. In fact, most of those consumers who switch outside the OEM channel in response to bundling would not actually be lost to Intel in terms of hardware sales. Outside the OEM channel they would combine an Intel CPU with any non-McAfee security software.[125] Depending on the assumptions on switching behaviour of end customers, a wide range of critical loss values can be obtained. For a reasonable range of such assumptions, the critical loss in the Commission's calculation,

---

123 McAfee achieves around [70-80]% of its total software security revenue in the endpoint security area. The consumer segment accounts for [50-60]% of revenues in the endpoint security area (in 2009 the total available market for endpoint security represented approximately USD [5-10] billion, of which USD [0-5] billion ([50-60]%) corresponded to the consumer segment). Approximately […]% of McAfee's revenues in the consumer segment are generated through the OEM sales channel, including new subscriptions and renewals. The Commission assumes that the distribution of revenues across segments for other security software vendors is similar to McAfee's. The OEM channel then represents approximately [10-20]% of the annual revenues of a security software firm.

124 The above mentioned [10-20]% share of potentially foreclosed revenues would materialize in the long-run, i.e. once SSVs would not be making revenues on renewals of software running on PCs which had been sold through the OEM channel before Intel started with commercial bundling. After Intel adopting such a strategy, SSVs could keep making revenues on subscription renewals of software running on PCs which were shipped before Intel would start applying a commercial bundling strategy. It would take time until this installed base deteriorates with older PCs gradually getting replaced. In the meantime a substantially smaller, but with time increasing share of the revenues of SSVs could be affected by commercial bundling.

125 In fact, in a response to this argument, Professor Timothy Bresnahan notes that "the customer is free to ignore the trial and choose whatever security software she wants from any distribution channel for security software. There is no reason that any foreclosure of this [the OEM] software channel would lead to consumers switching hardware vendors." ([…])

stemming from the loss of sales to OEM's, is higher than the critical loss submitted by Intel, but remains however limited.

276. To sum up, while under the Commission's approach for a reasonable range of assumptions the critical loss stemming from the loss of sales to OEM's is higher than the critical loss submitted by the notifying parties the economic analysis performed by both Intel and the Commission suggests that the critical loss remains limited. Accordingly, the incentives of Intel to engage into a commercial bundling might indeed be weakened by the risk of loosing CPU sales to OEMs.

4.3. Effects on markets

The notifying party's view

277. According to Intel and on the basis of the economic analysis detailed above, any foreclosure strategy could achieve no more than a [less than 1%] market share gain for McAfee. Even if Intel had an incentive to apply such a strategy, it could not foreclose enough sales to affect competition in endpoint security software. This would indeed still leave McAfee as a distant number two player in endpoint security software, with roughly the same [10-20]% of the overall security software market that it possessed before the acquisition.

278. In addition, Intel claims that any contractual tying arrangement is likely to be countered by McAfee rivals who may decide to price more aggressively to maintain market share, mitigating the effect of foreclosure. With AMD in Intel's market and with Symantec, Trend Micro and Kaspersky in McAfee's market, there remain effective single-product players in either market.

Results of the market investigation

279. The market investigation suggests that a commercial bundling alone can not have sufficiently strong foreclosure effects to lead to a significant impediment of competition in the security software or CPU markets. The main reason seems to be that already today the OEM distribution channel is almost exclusively reserved to Symantec, McAfee and Trend Micro.

280. For SSVs operating with a *freemium* model, as well as those which do not have access to the OEM channel, the merger will thus not lead to a deterioration of the current situation.

281. Some respondents indicate that some small SSVs could however exit the market. One of them indicates in particular that "[…] *several market participants are break-even or marginally profitable and could be driven from the market if such bundling strategy would be implemented successful.*"[126] According to one McAfee competitor, "*there is a danger that vendors will be forced out of the market because of the lost revenue from one of the main routes to market. This would probably not be an immediate effect but*

[126] Non-confidential reply to the Commission's market investigation.

would happen over a period of a couple of years as more and more people renew hardware."[127]

282. A few respondents to the market investigation raise further concerns. According to one McAfee competitor, "*although the OEM channel is one of two primary customer acquisition channels used by Symantec, the market share data clearly reveal that it is the critical channel for winning new business, since it is those ISVs that are present in the OEM channel that account for over 70% of consumer security software sales. Commercial bundling would foreclose this vital channel, resulting in the immediate and significant decline of the ISVs that sell through that channel and a significant detrimental impact on the industry as a whole*".[128]

283. Some respondents also suggest that the OEM channel is important for McAfee's main competitors' revenues and profitability and thus for their available R&D budget. They argue that since the three big vendors (Symantec, McAfee and Trend Micro) together account for about 70 % of the revenues in consumer endpoint security the foreclosure of Symantec and Trend Micro from the OEM channel could significantly reduce the overall available R&D funds in the security industry as a whole.

284. In addition, some respondents consider that the ability to react effectively is limited. According to one McAfee competitor, "*whilst* [it] *would consider a variety of options, none of the available strategies would be likely to prevent Intel eliminating competition in the security software market through implementing a commercial bundling strategy. Although* [*it*] *would try to defend its market share and growth by investing more heavily in marketing, even a radical increase in marketing investment would likely not offset the loss.*" According to another one, "*depending on the level of the implied discount,* [*it*] *would not be able to offer a competitive alternative (even in a partnership with a competitor of Intel).* [*It*] *would be forced to lower prices.*"[129]

Results of Commission assessment

285. First, it should be borne in mind that the possible effect of a commercial bundling strategy would concern only a very specific part of the endpoint security sector, that is consumer endpoint security shipped through the OEM channel, which represent only a relatively small share of security solutions shipped, and is a sale channel for a limited number of vendors only (essentially Symantec, McAfee and Trend Micro in commercially significant magnitude).

286. Second, very few respondents to the market investigation have argued that such a strategy would lead a majority of SSVs to exit the market, and many of them consider that it would have a marginal impact of SSVs such as *freemium* vendors.

287. Third, on the basis of the economic analysis detailed above, the Commission agrees that in the short run commercial bundling in the OEM channel is likely to affect a relatively small share of security software vendors' revenues, and exclusively the limited

---

127 Non-confidential reply to the Commission's market investigation.

128 Non-confidential reply to the Commission's market investigation.

129 Non-confidential reply to the Commission's market investigation.

number of SSVs present in the OEM channel as explained in paragraph 271. In the hypothetical scenario that Intel adopted such a strategy, SSVs could for some time rely on the renewals of subscriptions installed on PCs which were purchased before the bundling started. The potentially foreclosed share of revenues could later on increase with time. However, it should also be taken into account that during this period SSVs could develop strategies to adapt to Intel's strategy, for example by focusing on sales in the enterprise segment or via direct sales, the retail channel or internet service providers. Commercial bundling in isolation is not very likely to lead to a decrease in revenues for security software sales of a magnitude which would result in important players leaving the security software market or even a market segment.

288. The Commission therefore concludes that foreseeable effects of such a strategy would probably remain limited.

4.4 Conclusion

289. For the above mentioned reasons, the Commission therefore concludes that while the investigation has revealed Intel's ability to commercially bundle its hardware solutions with McAfee's security software solutions, the Commission's analysis comes to the result that there seem to be limited incentives to do so. The market investigation also suggests that possible antitrust enforcement would have a certain deterrent effect. Finally, foreseeable effects of such a strategy would also probably remain limited.

290. Taken in isolation the possibility of commercial bundling does therefore not give rise to serious doubts as to the compatibility of the transaction with the internal market.

291. However, the Commission considers that it is likely that together with a degradation of interoperability of Intel's chipsets/CPUs vis-à-vis McAfee competitors and/or a technical tie between the parties' products, a commercial bundling strategy could give rise to serious doubts as to the compatibility of the transaction with the internal market.

5. Assessment of a foreclosure strategy based on a combination of practices

292. Some respondents to the market investigation are concerned about the overall effects of a combination of technical tying or a degradation of interoperability together with commercial bundling that could lead, according to certain respondents to the market investigation, to (i) the exit of competitors from endpoint security markets[130] and (ii) the raise of barriers to entry to the endpoint security markets and/or chipset/CPU markets.[131]

293. While it does not appear that commercial bundling strategies in isolation pose a serious concern, they could reinforce the concerns raised by other foreclosure strategies, notably if the technical tying of McAfee's software solutions with Intel hardware makes OEMs more willing to accept commercial bundles.

294. In view of the above, the Commission considers that there are sufficient elements on the basis of which it would seem likely that Intel would have the ability to foreclose

130 9 out of 12 respondents to this question.

131 5 out of 12 respondents to this question.

McAfee competitors on the endpoint security markets and/or Intel competitors on the chipset/CPU markets by combining the above mentioned strategies.

295. The same conclusion can be reached with regards to Intel's incentives to enter in such combined strategies. It is also likely that the impacts of such combined strategies on the security solutions and/or chipset/CPU markets are at least identical to one of the three above-assessed strategies.

296. For the above reasons, the Commission concludes, also in the light of the results of the market investigation, that the likelihood of a combination of technical tying, interoperability hampering and/or commercial bundling will give rise to serious doubts as to the compatibility of the concentration with the internal market.

VI. COMMITMENTS SUBMITTED BY THE NOTIFYING PARTY

A. Description of the commitments initially submitted

297. In order to render the concentration compatible with the internal market, Intel submitted on 5 January 2011 a set of commitments.

298. According to this first set of commitments as regards interoperability concerns, and subject to the important limitation referred to in paragraph 299 below, Intel would in general ensure on an ongoing basis and in a timely manner that instructions and interoperability information for new functionalities in Intel CPUs and chipsets are documented and available for use by independent SSVs on a royalty-free basis.

299. However, Intel excluded from this interoperability commitment all technologies it would develop jointly post-transaction with McAfee.

300. As regards the interoperability of Intel endpoint security solutions with hardware developed by Intel competitors, Intel would not take affirmative steps to degrade its software performance when operating on a personal computer containing a non-Intel CPU.

301. As regards the Commission's technical tying concerns, in the case where Intel would add a malware detection engine to Intel CPUs and chipsets that are made commercially available prior to the third anniversary of the adoption of the Commission's decision, Intel would offer to license independent SSVs to interoperate with such malware detection engine such that the subscription services offered by such vendors would be able to utilize Intel’s malware detection engine. This would mean that the malware detection engine could still be integrated into the Intel hardware persistently and could not be switched off and/or replaced by McAfee competitors. However, it would be accessible by McAfee competitors, which could use this engine and try to combine it with other modules of their security solution (for instance interaction with their threat database based in the 'cloud'/the internet).

302. The enforcement of these commitments would be assured via a dispute settlement mechanism, including a fast-track dispute settlement procedure and arbitration.

303. These commitments would be effective worldwide and would remain in effect for five years (interoperability) and for three years (technical tying) from the closing of the transaction.

304. The Commission assessed the appropriateness of the commitments offered on 5 January 2011 in the light of the principles underlying its remedies policy and carried out a market test.

B. Compatibility with the remedies policy principles

305. From the outset, the Commission recalls that divestitures or the removal of links with competitors are the preferred remedy to eliminate certain competition concerns and that commitments relating to the future behaviour of the merged entity may be acceptable only exceptionally in very specific circumstances. In any case, divestitures are the benchmark for other remedies in terms of effectiveness and efficiency.

306. In the conglomerate case at stake, remedies other than divestiture remedies appear best suited to directly address the concerns raised. Indeed, this is a case where one of the main concerns is that control of key technology and possibly related IP rights may lead to foreclosure of competitors the products of which need to interoperate with this technology on an equal footing. The parties may withhold information necessary for the interoperability of competing security software or competing CPUs and chipsets, thus raising competition problems. In these circumstances, commitments to grant competitors access to the necessary information may eliminate the competition concerns.[132]

307. In those cases, commitments should foresee non-exclusive licences or the disclosure of information on a non-exclusive basis to all third parties which depend on the IP rights or information for their activities. It has to be further ensured that the terms and conditions under which the licenses are granted do not impede the effective implementation of such a license remedy. The terms and conditions should be clear and transparent. This also applies to the pricing or the commitment should take the form of royalty-free licences. The Commission will only accept such commitments if it can be concluded that they will be effective and competitors will likely use them.[133]

308. As regards the Commission's technical tying concern, SSVs need protection from bundling practices by which Intel would leverage its dominant position into the security solutions market. In particular, SSVs need to be in a position to disable security related features on the Intel platform so that these features do not interfere with the performance of the solutions.

309. As regards commercial bundling, as already indicated in paragraph 290, the Commission considers that taken in isolation commercial bundling does not give rise to serious doubts as to the compatibility of the transaction with the internal market. Therefore, provided that Intel proposes adequate remedies for the degradation of interoperability and for the technical tying concerns, it is not necessary that Intel proposes remedies for commercial bundling.

---

[132] Case COMP/M.3083 - GE/Instrumentarium, 2 September 2003, and case COMP/M.2861 - Siemens/Draegerwerk, 30 April 2003.

[133] Commission Notice on remedies — Guidelines on the application of Article 81 of the EC Treaty to technology transfer agreements, OJ C 101, 27.4.2004, p. 2, ("Commission Notice on remedies"), paragraph 63.

C. Outcome of the market test

1. Overall outcome

310. A large number of market participants supported the overall scope and nature of the commitments. Most respondents accepted that the competition concerns in this case could be solved with commitments on interoperability and technical tying.

311. Respondents generally also accepted that any commitments should only extend to areas where Intel has significant market power, that is to say CPUs and chipsets for servers, desktops, laptops, workstations and netbooks. Only few respondents requested commitments to also address the mobile and embedded segment, that is to say smartphones and other portable devices, where Intel has limited market power.

312. However, a significant number of respondents expressed strong and substantiated concerns on the design and the formulation of the proposed interoperability and technical tying commitments. The strongest concerns were expressed by the parties' competitors. A few OEMs also voiced concerns, albeit less strongly.

2. Interoperability

313. Many complainants considered that both the design and the formulation of the interoperability remedies submitted by Intel did not provide sufficient guarantees to ensure a genuine level playing field.

314. First, these respondents requested in particular to clearly state the objective of the interoperability remedy to ensure that the products of independent SSVs can fully interoperate with Intel hardware products on the basis of the same interoperability information as available to and on an equal footing with Intel/McAfee.

315. Second, the complainants indicated that the definitions used in a number of provisions have to be improved and clarified.

316. Third, these respondents required Intel to provide the Commission with drafts of the licence under which it intends to license the required documentation as well as the warranty that it will provide confirming the completeness and accuracy of the interoperability information. The terms of those clauses were considered as crucial for their effectiveness and it was considered necessary that they be market tested before the Commission authorises the deal.

317. Fourth, the complainants requested that access to the required interoperability information including patents and IP will be on a royalty-free basis and not subject to field of use restrictions.[134]

318. Fifth, these respondents asked for a commitment that Intel will not engineer or design Intel hardware products in any way that degrades the performance of either the computer containing the hardware or the endpoint security software where the security software is supplied by third parties.

---

134 Under a field of use restriction the licence is either limited to one or more technical fields of application or one or more product markets (cf. paragraph 179 of the Commission Notice on remedies).

319. Sixth, the complainants asked the Commission not to accept the exception to the interoperability obligations for innovation based on a material contribution from McAfee.

320. Finally, certain respondents requested a longer duration than five years and that new hardware features of Intel's competitors should also be supported by McAfee.

3. Technical tying of Intel hardware and McAfee security solutions

321. Certain participants to the market test voiced strong concerns on this remedy and in particular criticised the following:

322. First, the scope of the tying remedy would be too limited since it only covered a 'malware detection engine' and not other security technologies. Implicitly it would *de facto* allow Intel to bundle all other forms of endpoint security technologies. The term of 'malware detection engine' was also considered so vague that it would not be possible to enforce the remedy.

323. Second, the mechanism would not be a prohibition to bundle or not even an obligation to allow for replacements, but would merely provide for access from third parties to the tied malware engine. This mechanism would (1) impose on the market the Intel solution for the engine with a risk of monoculture and single point of failure on the engine and (2) force SSVs to adapt their malware detection technologies in the cloud to Intel's engine and (3) oblige the latter on top to pay for access to that engine. SSVs claim that they should at the very least have the possibility to replace the Intel engine with their own engine.

324. These market test participants that voiced concerns considered that the duration of the tying remedy of three years as too short.

325. One respondent requested a comprehensive undertaking by Intel not to bundle any endpoint security software technology with its hardware products for five years. Thereafter, Intel should make available to OEMs and end users a mechanism to enable them to fully replace any Intel security features and functions that it bundles with its hardware.

4. Enforcement provisions of the commitments

326. Market respondents considered enforcement provisions as important and highlighted significant shortcomings. They submitted that arbitration procedures, similar to litigation, entail risks of expensive and lengthy procedures. Complainants therefore requested:

- (i) a monitoring trustee with access to expertise and involved in initial period for bilateral dispute resolution before triggering arbitration;

- (ii) the arbitration court to provide preliminary ruling or final ruling within short and fixed timeframe (one or six months);

- (iii) reporting obligations for Intel;

- (iv) the Commission's optional involvement in an arbitration procedure.

327. A general basic condition for the Commission to accept commitments is that they must be implemented effectively. In light of the shortcomings identified during the market test, the Commission considers that the enforcement provisions were not sufficient to ensure effective implementation of the commitments.

5. Conclusion of the market test

328. The Commission considers that the concerns raised mainly by many of the competitors of Intel and McAfee - in particular with regard to interoperability, technical tying and enforcement - were appropriate and relevant and therefore conducted further discussions with Intel in order to address them.

329. As regards the interoperability commitments, the Commission finds that the total exclusion of interoperability obligations with regard to future innovation developed by McAfee or jointly McAfee/Intel would go too far. It considers that interoperability with Intel's future hardware inventions on a non-discriminatory basis is crucial for third party security software vendors to compete on a level playing field.

330. Regarding the duration of the interoperability commitments, the Commission notes firstly that the market test only revealed limited concerns. Secondly, the market investigation has shown that significant and continuous innovation is indispensable to effective security and that the security market is characterized by rapid innovation. The functionalities of the products may therefore significantly change within short time frames. The Commission therefore considers that a period of time of five years is sufficient and appropriate.[135][136]

331. The Commission considers that the points raised on the need for McAfee's solutions to actively support non-Intel hardware would go beyond the concerns identified by the Commission given that McAfee is not dominant on any of the relevant markets.

332. As regards the proposed tying commitment, given that Intel has not submitted and the Commission cannot see any objective reasons for a shorter duration than the duration of the interoperability commitment, the Commission considers that the duration of the tying remedy should be aligned on the interoperability remedy. On the one hand, the Commission considers that a total prohibition of all technological forms of technical tying of security software would be too intrusive because it would prevent innovation resulting from any combined new Intel/McAfee products. On the other hand, the Commission considers that the proposed commitment addressed the risk of monoculture only partially, since it only covered the subscription services portion of the potential tied security solutions. Moreover, the Commission considers that its scope might be too limited in light of the different possibilities for tying hardware and security software. Indeed, as already indicated in paragraphs 181 and *seq.* of the present decision, besides

---

[135] Commission Notice on remedies, paragraph 70: "*The Commission may accept that non-divestiture remedies are limited in their duration. The acceptability of a time limit and the duration will depend on the individual circumstances of a case and cannot be pre-defined in a general in a general manner in the present Notice*".

[136] For the sake of clarity, both during the validity and after expiry of the commitments, antitrust rules, in particular article 102 TFEU, continue to apply. Please see also paragraph 127 of the present decision.

the malware detection engine, there are several technological possibilities available for Intel to technically tie.

D. Final set of remedies

333. Following the communication to the notifying party of the outcome of the market test on the first set of commitments, Intel submitted revised sets of commitments on 17 and 19 January 2011.

334. The Commission conducted further discussions with Intel, as it appeared that they were still not addressing certain important and appropriate concerns raised by the market test.

335. In parallel to these discussions and after having received the penultimate set of commitments, the Commission carried out a limited market test[137]. It confirmed the significant progresses achieved in comparison with the set of commitments initially submitted on 5 January 2011 for the first market test, while some concerns were not considered as solved.

336. On the basis of such discussions, Intel offered an amended and final set of commitments on 20 January 2011, which now address all of the Commission's remaining concerns that gave rise to serious doubts as to the compatibility of the concentration with the internal market.

1. Interoperability

337. As regards the interoperability of its CPUs and chipsets, Intel substantially improved the commitments to address the outstanding contentious issues. Improvements include in particular the addition of guiding principles for the commitments and the clarification of various definitions (e.g. endpoint security, interoperability information).

338. More importantly, Intel agreed to remove the exception to the interoperability commitment for merger-specific innovations.

339. The Commission considers that these revised commitments submitted by Intel will ensure the necessary degree of interoperability of Intel hardware with non-McAfee security solutions.

340. As regards the interoperability of McAfee security solutions with non-Intel hardware, Intel gave a more precise definition to identify what would constitute a degrading of interoperability, which renders the commitment verifiable by a trustee. The Commission therefore considers the commitments submitted by Intel will ensure that no degradation of interoperability of McAfee software with non-Intel hardware will occur.

---

[137] The Commission held conference calls with one OEM and one SSV, which in light of their previous responses to questionnaires of the Commission appeared as particularly well informed about the functioning of the markets involved and as representative of the concerns expressed by market participants.

2. Technical tying of Intel hardware and McAfee security solutions

341. As regards the technical tying of Intel hardware and McAfee security solutions, Intel has substantially improved the commitments to address the contentious issues. Improvements concern notably:

- (i) a widening of the scope of the commitments that now include the adding of all endpoint security software to Intel CPUs and chipsets (instead of only the malware detection engine);

- (ii) an increase of the duration of this commitment to five years;

- (iii) 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 bundle or an obligation to effectively replace tied security – Intel commits to allow for the option to switch-off tied features. Therefore OEMs would have at least the option to replace them with security solutions provided by independent SSVs instead.

342. The Commission considers that the commitment submitted by Intel enables the effective disablement of any Intel security software features that it bundles with its hardware and that the quality of the performance of any alternative endpoint security software that is selected by OEMs or end users is in no way degraded by the replacement of the bundled Intel software. The Commission considers that this commitment is proportionate insofar as it does not prevent Intel/McAfee from offering on the market any combined new products but nevertheless contributes to avoid the risk of monoculture and to ensure continued competition and innovation amongst SSVs.

3. Enforcement provisions of the commitments

343. Intel has substantially improved the monitoring and enforcement provisions of the commitments. These provisions now include both a section on a monitoring trustee and a revised section on the dispute settlement procedure.

(1) Trustee

344. Intel now offers a monitoring trustee. As regards the trustee, the function, mandate and related provisions provided for in the commitments are essentially in line with the Commission standard requirements for commitments according to which the monitoring trustee must be in a position to act as the Commission's 'eyes and ears' to ensure the compliance of the parties with the commitments. Improvements include in particular the appointment of the monitoring trustee, its involvement in the initial bilateral dispute resolution before triggering arbitration, and a (limited) reporting obligation. Furthermore, Intel has committed not to close the notified transaction until twenty working days after the date of adoption of the present decision which should afford reasonable time to ensure the appointment of the monitoring trustee.

(2) Dispute Settlement Procedure

345. The commitments also provide for a dispute settlement mechanism, including a fast track arbitration procedure.

346. While the shortcomings of the initially proposed arbitration procedure were limited, Intel has further improved the provisions, notably with the following provisions:

- (i) the arbitration court may make a preliminary ruling within one month;
- (ii) the final ruling shall be rendered within six months;
- (iii) the Commission has the possibility to get involved in the arbitration procedure.

347. The Commission considers that the provisions now foreseen in the commitments are in line with its standard requirements that the trustee is able to assist in arbitral proceedings to the effect that these may be finalised in a short period of time.

(3) Standard agreements

348. Parts of these commitments will need to be implemented through agreements the terms and conditions of which do not form an integral part of the commitments but are the means by which they will be implemented in practice. These agreements and their terms and conditions will need to be consistent with the commitments to ensure their effectiveness and cannot include terms and conditions endangering their effective implementation. Intel has committed to a structured process for the Commission's approval of the standard texts for license and warranty agreements. More precisely, this structured process provides for the possibility for Intel to submit draft standard texts for the Commission's approval. If the Commission does not approve Intel's first proposal, Intel can make a second proposal. If the Commission does not approve the second proposal either, the Commission can instruct the monitoring trustee to recommend necessary modifications to the revised texts and approve them. For all these steps, leading to the approval of standard texts, a clear time-frame is defined in the commitments. The Commission will therefore have all ability to review, market test and approve these agreements within a short and clearly defined time frame following the adoption of the present decision.

349. The Commission considers that overall these elements will allow for an effective enforcement and ensure an effective implementation of the commitments.

4. Conclusion on the revised set of commitments

350. For the reasons outlined above, the commitments entered into by Intel are sufficient to eliminate the serious doubts as to the compatibility of the transaction with the internal market.

D. Conditions and obligations

351. Under the first sentence of the second subparagraph of Article 6(2) of the Merger Regulation, the Commission may attach to its decision conditions and obligations intended to ensure that the undertakings concerned comply with the commitments they have entered into vis-à-vis the Commission with a view to rendering the concentration compatible with the common market.

352. Where a condition is not fulfilled, the Commission’s decision declaring the concentration compatible with the internal market no longer stands. Where the undertakings concerned commit a breach of an obligation, the Commission may revoke

the clearance decision in accordance with Article 8(6) of the Merger Regulation. The undertakings concerned may also be subject to fines and periodic penalty payments under Articles 14(2) and 15(1) of the Merger Regulation.

353. In accordance with the distinction described above, all requirements set out in the commitments are considered to constitute obligations.

354. The Commission has concluded that the commitments submitted by Intel are sufficient to remove the serious doubts raised by the concentration. Accordingly, subject to the full compliance with the commitments submitted by Intel, the Commission has decided not to oppose the notified operation and to declare it compatible with the common market and with the EEA Agreement.

355. The detailed text of the commitments is annexed to this decision. The full text of the annexed commitments forms an integral part to this decision.

VII. CONCLUSION

356. For the above reasons, the Commission has decided not to oppose the notified operation as modified by the commitments and to declare it compatible with the internal market and with the functioning of the EEA Agreement, subject to full compliance with the obligations laid down in the commitments annexed to the present decision. This decision is adopted in application of Article 6(1)(b) in conjunction with Article 6(2) of Council Regulation (EC) No 139/2004.

For the Commission

(signed)
Joaquín ALMUNIA
Vice-President

COMMITMENTS TO THE EUROPEAN COMMISSION

In the event that the European Commission (the "Commission") is unable to conclude at the end of Phase I that the acquisition of McAfee, Inc. by Intel Corporation is compatible with the Common Market and the EEA Agreement by means of a decision without undertakings by Intel, Intel hereby provides the commitments specified below (the "Commitments") pursuant to Article 6(2) of Council Regulation (EC) No 139/2004 (the "Merger Regulation") in order to enable the Commission to adopt a decision pursuant to Article 6(1)(b) of the Merger Regulation.

These Commitments shall take effect upon receipt of the Decision and shall be binding on Intel (as defined below). These Commitments are offered exclusively in the context of the concentration between Intel and McAfee and are without prejudice to the position of Intel and/or its subsidiaries in future cases examined by the European Commission.

This text shall be interpreted in the light of the Decision to which these Commitments are attached as conditions and obligations, and in the general framework of Community law, in particular in the light of the Merger Regulation, and by reference to the Commission Notice on remedies acceptable under the Council Regulation (EC) No 139/2004 and under Commission Regulation (EC) No 802/2004.

Section A. Definitions

1. For the purpose of the Commitments, the following terms shall have the following meaning:

Effective Date means the date of the adoption of the Decision.

Endpoint Security Software means client antivirus products, file/storage server antivirus, client antispyware products, personal firewall products, host intrusion prevention products, file/disk encryption, anti-spam, content filtering, and endpoint information protection and control products that are intended to run on an Intel microprocessor and intended for use on a Personal Computer.

Intel means Intel Corporation (and McAfee, Inc. after the completion of the McAfee acquisition) and companies and/or affiliated businesses controlled by these entities.

Intel Mainstream Microprocessors or Chipsets means x86 microprocessors and related chipsets that are promoted by Intel for use in a Personal Computer.

Intel's McAfee Subsidiary means the Intel organization that comprises or is the successor to McAfee, Inc.

Instruction, Interoperability, and Optimization Information means the information necessary to develop and optimize Endpoint Security Software that effectively utilizes functionality in Intel Mainstream Microprocessors or Chipsets utilized by Endpoint Security Software sold or licensed by Intel (including Endpoint Security Software sold or licensed by Intel's McAfee Subsidiary). Instruction, Interoperability, and Optimization Information shall include information that is equivalent to the type of information provided to third party vendors of Endpoint Security Software prior to Intel's acquisition of McAfee, such as in the *Intel® 64 and IA-32 Architectures Software Developer's Manual* and the *Intel® 64 and IA-*

32 Architectures Optimization Reference Manual available at http://www.intel.com/products/ processor/manuals/, and shall include but not be limited to: (i) the operands required by instructions and their encodings; (ii) the opcodes associated with the instruction and their encodings; (iii) the valid modes of operation; (iv) any side-effects not covered in the basic functionality that are exposed to software, including effects on external hardware; (v) any designed exceptions that an instruction can cause that result in calling an error handler, and under what conditions and in which modes of operation they can occur; and (vi) execution timings where relevant. Provided, however, that Instruction, Interoperability, and Optimization Information shall not include (x) information relating to the manner in which Intel implements the underlying functionality in its microprocessors and chipsets; or (y) information relating to Intel's implementation of such functionality in Endpoint Security Software.

Personal Computer means any desktop, laptop, netbook, notebook, workstation or server computer; provided, however, that no smart phone, cell phone, tablet, Pocket PC or other device shall be considered a Personal Computer.

Required Documentation means the documentation required by paragraph 4.a of these Commitments.

Timely Manner means one year before the planned commercial availability to end users of an Intel Mainstream Microprocessor or Chipset for which Intel must provide Required Documentation.

Section B. Commitments

2. Intel understands that the Commission is concerned that, as a result of the proposed acquisition of McAfee by Intel, non-McAfee security software may suffer from a lack of interoperability with Intel microprocessors and chipsets or from technical tying between the latter and McAfee's security software. Intel also understands that the Commission is concerned about possible effects on Intel's competitors if McAfee software is no longer compatible with non-Intel microprocessors and chipsets.

3. Pursuant to the commitments in paragraphs 4 and 5 below, Intel intends that, following its acquisition of McAfee, third party vendors of Endpoint Security Software will have access to Instruction, Interoperability, and Optimization Information that will enable their software to utilize the functionality of Intel Mainstream Microprocessors or Chipsets in the same way as that functionality is utilized by Endpoint Security Software sold by Intel. Pursuant to the commitments in paragraphs 6 and 7, Intel does not intend that there will be impediments to the operation of Endpoint Security Software sold by vendors other than Intel when running on Intel Mainstream Microprocessors or Chipsets. Pursuant to Paragraph 8, Intel also does not intend that there will be impediments to the operation of Intel Endpoint Security Software when running on Personal Computers containing microprocessors or chipsets sold by vendors other than Intel.

4. Intel makes the following commitments to address the Commission's concerns:

a. Subject to the limitations set forth herein, Intel shall ensure on an ongoing basis and in a Timely Manner that Instruction, Interoperability, and Optimization Information is documented and available for use by third party vendors of Endpoint Security Software.

b. The Required Documentation will be provided to any third party vendor of Endpoint Security Software that requests such access pursuant to a license, non-disclosure agreement, or other suitable contractual agreement, the terms of which shall be royalty-free and which may include a requirement that the licensee maintain the confidentiality of information provided by Intel. Provided, however, that nothing herein shall require Intel to provide the Required Documentation to any third party more than one year before the planned commercial availability of a new Intel Mainstream Microprocessor or Chipset incorporating features that are the subject of the Required Documentation.

c. The Required Documentation will be as complete and accurate as that provided to third party vendors of Endpoint Security Software prior to Intel's acquisition of McAfee. Intel will provide a warranty to that effect.

d. Intel shall dedicate no fewer than ten full time equivalent software engineers, exclusive of any engineering support provided to Microsoft and McAfee, to assist third party vendors of Endpoint Security Software in implementing Intel technologies. Intel shall have the right to use commercially reasonable criteria for allocating these resources among such vendors, including without limitation criteria based on each vendor's need for and utilization of such resources, and Intel may require any vendor to which it provides such support to pay reasonable fees in consideration for such support.

e. Intel shall provide to any third party vendor of Endpoint Security Software any software development kit supporting a microprocessor instruction or chipset feature disclosed in the Required Documentation when such development kit is made available to multiple independent software developers. For the avoidance of doubt, disclosure to operating system vendors shall not trigger any disclosure obligations under this paragraph.

5. Nothing herein shall limit Intel's ability to alter an instruction or function or the manner in which an instruction or function is accessed by software in order to correct bugs or other implementation issues at any time so long as Intel updates the Required Documentation in the same manner in which it updated such information prior to Intel's acquisition of McAfee.

6. If Intel adds Endpoint Security Software to Intel Mainstream Microprocessors or Chipsets and the presence or operation of such Endpoint Security Software would interfere with the effective operation of Endpoint Security Software then sold by a vendor other than Intel, Intel shall disclose technological means by which the Intel Endpoint Security Software may be disabled so that it does not interfere with such Endpoint Security Software then sold by a vendor other than Intel. Intel may require that any OEM that disables Endpoint Security Software supplied by Intel clearly and prominently disclose that such Endpoint Security Software has been disabled. For the avoidance of doubt, Intel shall have no obligation to disclose technological means that would disable: (i) individual microprocessor instructions; (ii) any firmware or other functionality incorporated in a microprocessor or chipset for the purpose of protecting such microprocessors or chipsets themselves from malware (as opposed to protecting a Personal Computer containing such microprocessors or chipsets from malware); or (iii) any firmware or other functionality incorporated in a microprocessor or chipset that also has a substantial application in software in addition to Endpoint Security Software.

7. Intel will not actively engineer or design Intel Mainstream Microprocessors or Chipsets to degrade the performance of Endpoint Security Software sold by a firm other than Intel. Intel shall not be deemed to have degraded the performance of Endpoint Security Software sold by a firm other than Intel if any impact on such software is a necessary byproduct of engineering or design changes that provide an actual benefit or improvement to Intel microprocessors or chipsets. Nothing herein shall require Intel to engineer or design Intel Mainstream Microprocessors or Chipsets to optimize the performance of Endpoint Security Software sold by a firm other than Intel.

8. Intel will not actively engineer or design Intel Endpoint Security Software to degrade its performance when operating on a Personal Computer containing a microprocessor not supplied by Intel. Intel shall not be deemed to have degraded the performance of Intel Endpoint Security Software if any impact on such software when operating on a Personal Computer containing a microprocessor not supplied by Intel is a necessary byproduct of engineering or design changes that provide an actual benefit or improvement to such software. Nothing herein shall require Intel to optimize McAfee Endpoint Security Software to utilize features of non-Intel microprocessors that differ from the implementation of such features in Intel microprocessors.

9. The following procedures shall apply with regard to approval of a form Non-Disclosure and Permitted Use Agreement (the "Form Agreement"):

a. Intel shall submit to the Commission and the Monitoring Trustee no later than 5 working days after the appointment of the Monitoring Trustee a Form Agreement containing the applicable non-disclosure arrangements for the Required Documentation, the warranty referred to in paragraph 4.c, and the royalty-free license referred to in paragraph 4.b. The Form Agreement shall contain terms and conditions that implement these Commitments and that are consistent with the terms and conditions pursuant to which Intel disclosed confidential information to vendors of Endpoint Security Software prior to its acquisition of McAfee ("Prior Terms").

Nothing in the Form Agreement shall expand Intel's Commitments or provide remedies not contained herein.

b. Intel shall annex to the draft Form Agreement a Memorandum showing it is consistent with the Commitments and include certified copies of the Prior Terms.

c. The Commission shall verify that the draft Form Agreement is consistent with the Commitments. To assist the Commission the Monitoring Trustee shall submit a reasoned opinion within 5 working days, with a copy to Intel. If the Commission approves, it shall inform Intel in writing of the Commission's decision.

d. Should the Commission consider the draft Form Agreement is not consistent with the Commitments it shall inform Intel by letter of its reasons.

e. Within 10 working days Intel shall then submit a revised draft Form Agreement. The Monitoring Trustee shall submit a reasoned opinion on the revised draft Form Agreement within 5 working days, with a copy to Intel.

f. Should the Commission determine that the revised Form Agreement is not consistent with the Commitments, it shall inform Intel thereof and of the reasons for its determination and instruct the Trustee to recommend modifications to the revised Form Agreement necessary so that it will be consistent with, and solely to implement, the Commitments and in particular observing the terms referred to in paragraph 9.a. Intel shall have 5 working days to make its views known on the Trustee's recommendation draft. Hereafter the Commission may approve the Form Agreement and shall inform Intel in writing of its decision.

g. As soon as approved by the Commission, this Form Agreement shall be made available on the Intel website. Intel commits that it shall be prepared to execute an agreement, substantially in the form of the approved Form Agreement, with any third party entitled to access to Required Documentation under these Commitments. Any change to the Form Agreement shall be submitted to the Commission for approval.

h. Prior to the approval by the Commission of the Form Agreement, vendors of Endpoint Security Software shall be able to have access according to Prior Terms.

Section C. Monitoring Trustee

C.1. Appointment

10. Intel shall appoint a Monitoring Trustee to carry out the functions specified in paragraph 18 below. The Monitoring Trustee shall be independent of Intel, possess the necessary experience, competence and qualifications to carry out its mandate, and shall neither have nor become exposed to a conflict of interest. In particular, the Monitoring Trustee shall be familiar with the design and implementation of microprocessor technology.

11. The Monitoring Trustee shall be remunerated by Intel in a way that does not impede the independent and effective fulfillment of the Monitoring Trustee's mandate.

Proposal by Intel

12. No later than two weeks after the Effective Date, Intel shall submit a list of one or more persons whom Intel proposes to appoint as the Monitoring Trustee to the Commission for approval. The proposal shall contain sufficient information for the Commission to verify that the proposed Monitoring Trustee possesses the technical qualifications set out in paragraph 10 and shall include:

a. the full terms of the proposed mandate, which shall include all provisions necessary to enable the Monitoring Trustee to fulfill its duties under these Commitments;

b. the outline of a work plan, which shall describe how the Monitoring Trustee intends to carry out its duties under these Commitments.

Approval or rejection by the Commission

13. The Commission shall have the discretion to approve or reject the proposed Monitoring Trustee(s) and to approve the proposed mandate subject to any modifications it deems necessary for the Monitoring Trustee to fulfill its obligations. If only one name is approved, Intel shall appoint or cause to be appointed the individual or institution concerned as Monitoring Trustee, in accordance with the mandate approved by the Commission. If more than one name is are approved, Intel shall be free to appoint the Trustee from among the

names approved. The Monitoring Trustee shall be appointed within one week of the Commission's approval, in accordance with the mandate approved by the Commission.

New proposal by Intel

14. If all the proposed Monitoring Trustees are rejected, Intel shall propose at least two more candidates within two weeks of being informed of the rejection, in accordance with the requirements and procedure set out in paragraph 12

Monitoring Trustee nominated by the Commission.

15. If all further proposed Monitoring Trustees are rejected by the Commission, the Commission shall nominate a Monitoring Trustee, whom Intel shall appoint, or cause to be appointed, in accordance with a trustee mandate approved by the Commission. In any event, this Monitoring Trustee shall also possess the technical qualifications set forth in paragraph 10.

16. So as to afford reasonable time for the appointment of a Monitoring Trustee pursuant to the procedures described in paragraphs 12 through 15, Intel commits not to close the notified transaction until twenty working days after the Effective Date.

C.2. Functions of the Monitoring Trustee

17. The Monitoring Trustee shall assume its specified duties in order to ensure compliance with these Commitments. The Commission may, on its own initiative or at the request of the Trustee or Intel, give any orders or instructions within the scope of the Trustee's mandate.

The Monitoring Trustee will act on behalf of the Commission as a trusted expert in the fast track dispute settlement procedure described in paragraphs 28 to 46 below.

Mandate of the Monitoring Trustee

18. The Monitoring Trustee shall:

a. broker a resolution of any dispute that would arise between a third party and Intel regarding compliance with the conditions and obligations attached to the Decision;

b. advise and, if need be, make written recommendations to the Commission as to Intel's compliance with the conditions and obligations attached to the Decision when any dispute between a third party and Intel regarding such compliance would be brought before the Arbitral Tribunal referred to in paragraph 32 below;

c. provide to the Commission, sending Intel a non-confidential copy at the same time, a report on 31 December of every year during the term of the Commitments as indicated in paragraph 49, regarding the status and outcome of any dispute between a third party and Intel in which the Monitoring Trustee has participated;

d. propose to Intel such measures as the Monitoring Trustee considers necessary to ensure Intel's compliance with the Commitments;

e. promptly report in writing to the Commission, sending Intel a non-confidential copy at the same time, if it concludes on reasonable grounds that Intel is failing to comply with the Commitments.

19. The Monitoring Trustee shall provide a detailed work plan to the Commission within one month of its appointment, sending a copy to Intel at the same time, describing how it intends to carry out its mandate.

20. The documents provided for in paragraphs 18 and 19 shall be prepared in English.

21. Subject to proper confidentiality provisions, Intel shall provide the Monitoring Trustee with such co-operation, assistance and information, including copies of all relevant documents and access to relevant staff, as the Monitoring Trustee may reasonably require in carrying out its mandate.

22. In carrying out its mandate, the Monitoring Trustee shall have due regard for Intel's legitimate interests in avoiding unjustified burden and interference in Intel's business operations.

23. Intel shall indemnify the Monitoring Trustee and its employees and agents (each an "Indemnified Party") and hold each Indemnified Party harmless against, and hereby agrees that an Indemnified Party shall have no liability to Intel for any liabilities arising out of the performance of the Monitoring Trustee's duties under the Commitments, except to the extent that such liabilities result from the willful default, recklessness, gross negligence or bad faith of the Trustee, its employees, agents or advisors.

24. At the expense of Intel, the Monitoring Trustee may appoint advisors, subject to Intel's approval (this approval not to be unreasonably withheld or delayed) if the Monitoring Trustee reasonably considers the appointment of such advisors necessary or appropriate for the performance of its duties and obligations under the Mandate, provided that any fees and other expenses incurred by the Monitoring Trustee are reasonable. Should Intel refuse to approve the appointment of advisors or any individual advisor proposed by the Monitoring Trustee, the Commission may approve the appointment of such advisors instead, after having heard Intel. Only the Monitoring Trustee shall be entitled to issue instructions to the advisors. Paragraph 23 shall apply mutatis mutandis.

C.3. Replacement, discharge and re-appointment of the Monitoring Trustee

25. If the Monitoring Trustee ceases to perform its functions under the Commitments or for any other good cause, including its exposure to a conflict of interest:

a. the Commission may, after hearing the Monitoring Trustee, require Intel to replace the Monitoring Trustee; or

b. Intel, with the prior approval of the Commission, may replace the Monitoring Trustee.

26. If the Monitoring Trustee is removed according to paragraph 25, the Monitoring Trustee may be required to continue in its function until a new Monitoring Trustee is in place to whom the Monitoring Trustee has affected a full hand-over of all relevant information. The new Monitoring Trustee shall be appointed in accordance with the procedure referred to paragraphs 10 to 15.

27. Besides the removal according to paragraph 25, the Monitoring Trustee shall cease to act as Monitoring Trustee only after the Commission has discharged it from its duties after all the Commitments with which the Monitoring Trustee has been entrusted have lapsed. However, the Commission may at any time require the reappointment of the Monitoring Trustee if it subsequently appears that the Commitments might not have been fully and properly implemented.

Section D. Fast track dispute resolution

28. In the event that a third party, showing a sufficient legitimate interest, claims that Intel is failing to comply with its obligations arising from these Commitments, such third party may invoke the dispute settlement procedure described in this Section.

29. The third party who seeks to initiate the procedure shall notify Intel and the Monitoring Trustee of its request and specify the reasons why it believes that Intel is failing to comply with the Commitments. Intel shall use its best efforts to resolve all differences of opinion and to settle all disputes of which it has been notified through co-operation and consultation within a reasonable period of time not to exceed fifteen working days after receipt of the request.

30. The Monitoring Trustee shall present its own proposal for resolving the dispute within eight working days, specifying in writing the action, if any, to be taken by Intel in order to ensure compliance with the Commitments vis-à-vis the third party, and be prepared, if requested, to facilitate the settlement of the dispute.

31. Should Intel and the third party fail to resolve their differences of opinion through co-operation and consultation, the third party may initiate the arbitration process described below. The arbitration process shall be used only to resolve disputes regarding compliance with the Commitments.

32. To initiate the arbitration process, the third party shall give written notice to Intel nominating an arbitrator and stating the specific nature of the claim, the factual basis of its position and the relief requested. Intel shall appoint another arbitrator within fourteen calendar days after receipt of the written notice. The arbitrators so appointed shall appoint a third arbitrator to be president of the arbitral tribunal within seven calendar days after both arbitrators have been nominated. Should Intel fail to nominate an arbitrator, or if the two arbitrators fail to agree on the president, the default appointment(s) shall be made by the International Chamber of Commerce (“ICC”). All three arbitrators shall have experience in the area of microprocessor technology. The three-person arbitral tribunal shall herein be referred to as the “Arbitral Tribunal”.

33. The dispute shall be finally resolved by arbitration under the ICC Rules of Arbitration, with such modifications or adaptations as foreseen herein or necessary under the circumstances (the “Rules”). The arbitration shall be conducted in London, England, in the English language.

34. The procedure shall be a fast-track procedure. For this purpose, the Arbitral Tribunal shall shorten all applicable procedural time-limits under the Rules as far as appropriate in the circumstances.

35. The Arbitral Tribunal shall, as soon as practical after the confirmation of the Arbitral Tribunal, hold an organisational conference to discuss any procedural issues with the parties to the arbitration. Terms of Reference shall be drawn up and signed by the parties to the arbitration and the Arbitral Tribunal at the organisational meeting or thereafter and a procedural time-table shall be established by the Arbitral Tribunal. An oral hearing shall, as a rule, be established within two months of the confirmation of the Arbitral Tribunal.

36. In order to enable the Arbitral Tribunal to reach a decision, it shall be entitled to request any relevant information from Intel or the third party, to appoint experts and to examine them at the hearing, and to establish the facts by all appropriate means. The Arbitral Tribunal is also entitled to ask for assistance by the Monitoring Trustee in all stages of the procedure if the parties to the arbitration agree.

37. The arbitrators shall agree in writing to keep any confidential information and business secrets disclosed to them in confidence. The Arbitral Tribunal may take the measures necessary for protecting confidential information in particular by restricting access to confidential information to the Arbitral Tribunal, the Monitoring Trustee and outside counsel and experts of the opposing party.

38. The burden of proof in any dispute governed under the Rules shall be borne as follows: (i) the party who has requested the arbitration must produce evidence of a prima facie case; (ii) if that party does so, the Arbitral Tribunal must find in favour of the requesting party unless Intel can produce evidence to the contrary.

39. The Commission shall be allowed and enabled to participate in all stages of the procedure by:

a. receiving all written submissions (including documents and reports, etc.) made by the parties to the arbitration;

b. receiving all orders, interim and final awards and other documents exchanged by the Arbitral Tribunal with the parties to the arbitration (including Terms of Reference and procedural time-table);

c. filing any Commission amicus curiae briefs; and

d. being present at the hearing(s) and being allowed to ask questions to parties, witnesses and experts.

The Arbitral Tribunal shall forward, or shall order the parties to the arbitration to forward, the documents mentioned to the Commission without delay.

40. In the event of disagreement between the parties to the arbitration regarding the interpretation of the Commitments, the Arbitral Tribunal shall inform the Commission and may seek the Commission’s interpretation of the Commitments before finding in favour of any party to the arbitration and shall be bound by the interpretation.

41. The Arbitral Tribunal shall decide the dispute on the basis of the Commitments and the Decision. The Commitments shall be construed in accordance with the Merger Regulation, EU law and general principles of law common to the legal orders of the Member States without a requirement to apply a particular national system. The Arbitral Tribunal shall take all decisions by majority vote.

42. Upon request of the third party, the Arbitral Tribunal may make a preliminary ruling on the Dispute. The preliminary ruling shall be rendered within one month after the confirmation of the Arbitral Tribunal, shall be applicable immediately and, as a rule, remain in force until a final decision is rendered.

43. The Arbitral Tribunal shall, in the preliminary ruling as well as in the final award, specify the action, if any, to be taken by Intel in order to comply with the Commitments vis-à-vis the third party (e.g. specify a contract including all relevant terms and conditions). The final award shall be final and binding on the parties to the arbitration and shall resolve the dispute and determine any and all claims, motions or requests submitted to the Arbitral Tribunal. The arbitral award shall also determine the reimbursement of the costs of the successful party and the allocation of the arbitration costs. In case of granting a preliminary ruling or if otherwise appropriate, the Arbitral Tribunal shall specify that terms and conditions determined in the final award apply retroactively.

44. The final award shall, as a rule, be rendered within six months after the confirmation of the Arbitral Tribunal. The time-frame shall, in any case, be extended by the time the Commission takes to submit an interpretation of the Commitments if asked by the Arbitral Tribunal.

45. The parties to the arbitration shall prepare a non-confidential version of the final award, without business secrets. The Commission may publish the non-confidential version of the award.

46. Nothing in the above-described arbitration procedure shall affect the powers of the Commission to take decisions in relation to the Commitments in accordance with its powers under the Merger Regulation and the Treaty on the Functioning of the European Union.

Section E. General provisions

47. If the acquisition of McAfee by Intel is abandoned, unwound or otherwise terminated, these Commitments shall automatically cease to apply.

48. If the approval of the Concentration by another governmental authority is made subject to requirements that are potentially inconsistent with these Commitments, Intel may request a review and adjustment of these Commitments in order to avoid such inconsistencies.

49. These Commitments shall be effective worldwide and shall remain in effect for five years from the Effective Date.

Section F. Review

50. The Commission may, where appropriate, in response to a request from Intel showing good cause and accompanied by a report from the Monitoring Trustee, waive, modify or substitute, in exceptional circumstances, one or more of the undertakings in these Commitments.