Intellectual Property Office

BL O/198/17

24 April 2017

PATENTS ACT 1977

APPLICANT	F Secure Corporation
ISSUE	Whether patent application GB1312856.6 complies with sections 1(1)(a), 14(3) and 14(5)
HEARING OFFICER	Dr. L. Cullen

DECISION

Introduction

1 This decision concerns patent application GB1312856.6 entitled "*Malware detection*", and whether it meets the requirements of section 1(1)(a), regarding novelty, and section 14, regarding support and sufficiency, of the Patents Act 1977 (the 'Act'). The application was filed under the provisions of the Patent Cooperation Treaty (PCT) on 5 January 2012, claiming an earliest priority date of 21 January 2011 and was initially published as WO2012/098018 on 26 July 2012. On entering the GB national phase, it was subsequently re-published as GB2502715A on 4th December 2013.

2 Throughout the examination process, the examiner remained of the view that the claimed invention was not novel over the disclosure in GB2463467A and that claim 1 was unclear. With the situation unresolved after multiple rounds of examination and argument, the applicant asked to be heard and the matter came before me at an oral hearing on the 16 January 2017. The applicant was represented by Dr. Robert Lind, assisted by Martin Bell, of Marks and Clerk LLP. Also present were the examiner, Manolis Rovilos, and the Hearing Officer's assistant, Emma Porter. There was one observer present for training purposes.

The Invention

3 The invention concerns a process for selecting the most appropriate method for detecting the presence of malicious software, referred to as malware, in computer files.

4 Different methods for detection of malware can be used to identify if such malicious software is present in particular computer files. Scanning each computer file in a system for malware takes time and consumes significant amounts of processor power. As a consequence, it is important to be able to select the most suitable method for malware detection, based on the information that can be most easily accessed from the computer file.

5 The term ‘malware detection processing’ is used to refer to any method or step that can be used to search for and actively identify malware.

6 Each malware detection processing method will use certain data from a computer file to carry out the malware detection and a scan for the presence of such file data can be used as a key or signpost to indicate that a particular malware processing method could be implemented, i.e. used, to actually determine if malware is present. As a result, determining if certain file data is present in a computer file is a means by which one can determine whether or not a malware detection processing method can be selected or not – if such file data is present, the related malware detection processing method could be used, if it is not, then it cannot be used.

7 The current version of independent claim 1 of the application, as amended on 19 July 2016, reads:

> *A method of processing a plurality of files to determine whether each of said files comprises malware, where a plurality of malware detection processing methods are available, the method comprising:*
>
> *a) selecting a file for processing;*
>
> *b) obtaining first data relating to said selected file;*
>
> *c) determining whether, based on the first data, a malware detection processing method can be selected from said plurality of malware detection processing methods and selecting a malware detection processing method to be applied to said selected file based upon said first data if it is determined that a malware detection processing method can be selected based upon the first data;*
>
> *d) if it is determined that, based upon the first data, a malware detection processing method cannot be selected, obtaining second data relating to said selected file and determining whether a malware detection processing method can be selected from said plurality of malware detection processing methods based upon a combination of said first and second data and if so selecting a malware detection method;*
>
> e) *if a malware detection processing method cannot be selected at step d), repeating that step one or more times to obtain at each step further data relating to the file and at each step determining whether a malware detection processing method can be selected from said plurality of malware detection processing methods based upon a combination of all the obtained data and if so selecting a malware detection method;*
>
> *and*
>
> f) *applying the selected malware detection processing method to said selected file.*

8 Thus the method of the application includes obtaining first data from a file to be scanned for malware, and using the first data to determine whether a method for malware detection can be selected from the various such methods available. If it is possible to select a suitable malware detection processing step using this first data, then this is step is selected for that computer file; however if a method of malware detection cannot be selected based on this first data alone, then second data is obtained from the file to be scanned; the first and second data are used in combination to determine if a method of malware detection can be selected. If so, the identified malware detection method is applied. If not, further data from the file to be scanned is obtained – third data - and combined with the first and second data, and the combined data is used to determine if a method of malware detection can be selected.

Written submissions after the hearing

9 In order to decide whether the application in suit was novel over the prior art as represented by GB2463467A (hereafter GB467), it was first necessary to construe the claims of the application to determine what are the essential features of the invention as claimed. At the hearing, it became clear that there was a difference between how the applicant considered the claims of the application should be construed in the light of the description as filed and how the examiner considered they should be construed. Given the importance that was placed on the construction proposed by the applicant as a means to overcome the novelty objection raised by the examiner, the topic of how the claims of the application should be construed was discussed at some length at the hearing.

10 Following the hearing, in an official letter dated 24 January 2017, the Hearing Officer asked the applicant to confirm, in writing, where in the application as filed there was the support for the claim construction they had proposed at the hearing; specifically, the applicant was asked to show that the two differences identified as part of the invention in the hearing were disclosed in the description as originally filed.

11 Written submissions from the applicant were received in response to this request on 20 February 2017 and these have been fully taken into account as part of my decision below.

Issues to be decided

12 There are two issues to be decided in relation to this application.

(i) Firstly, does the application in suit, as claimed in claims 1-8 currently on file, meet the requirement for novelty according to section 1(1)(a) of the Act over the disclosure in GB467, which is some of the applicants own prior art?

(ii) Secondly, and following on from the discussion of novelty and the construction of the claims proposed by the applicant to overcome the novelty objection, are the claims as construed supported by the description, as required under section 14(5) of the Act, and is the invention disclosed, as required under

section 14(3) of the Act, in a manner which is clear enough and complete enough to be performed by a person skilled in the art.

The Relevant Law

13 The relevant parts of the Act with respect to novelty are set out in section 1(1)(a) and section 2, which read as follows:

> *1.- (1). A patent may be granted only for an invention in respect of which the following conditions are satisfied, that is to say:*
>
> *(a) the invention is new;*
> *(b) ...;*
> *(c) …;*
> *(d) ….*

and

> *2.- (1). An invention shall be taken to be new if it does form part of the state of the art.*
>
> *(2). The state of the art in the case of an invention shall be taken to compromise all matter (whether a product, a process, information about either, or anything else) which has at any time before the priority date of that invention been made available to the public (whether in the United Kingdom or elsewhere) by written or oral description, by use or in any other way.*
>
> *……..*

14 Section 14 of the Act, entitled '*Making of Application*', sets down a number of requirements for a patent application. Sections 14(3) and 14(5)(c) relate to the specification and the claims respectively and read as follows:

> *……*
>
> *(3) The specification of an application shall disclose the invention in a manner which is clear enough and complete enough for the invention to be performed by a person skilled in the art.*
>
> *……*
>
> *(5) The claim or claims shall –*
>
> *(a) …;*
> *(b) …;*
> *(c) be supported by the description; ..*
> *(d) ….*

Argument and Analysis

15 In my analysis below, I will use the term 'malware detection processing' to refer to any method or step that can be used to search for and actively identify malware. I will make a distinction between the process of ***selecting*** a malware detection processing method and the process of ***implementing*** a malware detection processing method, i.e. the former is about identifying which malware detection processing method to use but does not include actually carrying out the malware detection processing step. The latter occurs after the malware detection processing method has been selected, and refers to the step of actually carrying out the malware detection processing method and obtaining a result to show that malware is or is not present.

Novelty

16 The examiner objects to all the claims of the application (see claims 1-8 as filed 19 July 2016), on the grounds that they lack novelty with respect to the disclosure of GB467 – see, for example, official examination report dated 7 September 2016 and official letter dated 4 November 2016[1].

17 GB467 discloses a method for scanning files for malware comprising first determining if a given electronic file has a valid digital signature; if it does have such a digital signature, then it verifies that this signature belongs to a trusted source. If it is found that it does belong to a trusted source, then no malware scan is performed on the electronic file. If a given electronic file does not have a digital signature, or if it does, but this digital signature does not belong to a trusted source, then the malware scan is performed.

18 The examiner argued that the malware processing method of GB467 comprises all the elements of the method for selection of a malware processing method as claimed in the application in suit. Selection of a file for digital processing according to GB467 involves obtaining first data with respect to the file (a valid digital signature; see page 8, lines 1-3), and based on the first data determining whether a malware detection processing method (the "checking for a valid digital signature against trusted keys" or "no scan" method; page 8, lines 2-7) can be applied. If it is determined that the first method cannot be applied, second data (a cryptographic hash of the file; page 9, lines 5-9) is obtained and a second method ("checking a cryptographic hash of the file"; page 9, lines 16-21) is used. If the second method cannot be used, then third data (the whole file) is obtained and a third method ("conventional scanning technique"; page 10, lines 8-11) is used to determine whether the selected file contains malware. The method disclosed in GB467 is implemented by a computer (see e.g. figure 1 and claim 1), and it thus anticipates claims 1 and 6-8.

19 The examiner also argued that according to the method taught in GB467, the first data is a digital signature (i.e. metadata associated with the file), which does not require reading data from the file itself in order to be obtained or processed. The second data

[1] See documents for the application in suit on the IPO's IPSUM database at https://www.ipo.gov.uk/p-ipsum/Case/ApplicationNumber/GB1312856.6

is a cryptographic hash of the file that does require reading data from the file. It is also implicitly disclosed that obtaining the second data takes a longer time than obtaining the first data (reading or processing a digital signature or the file header is less computationally complicated than processing the whole file to calculate the hash value); therefore claims 2-5 are also anticipated by GB467.

20 During the hearing the applicant was asked to explain how the claimed invention differed from the malware detection processing method detailed in GB467.

21 The first difference identified by the applicant between the claimed invention and the method disclosed in GB467, was the stepwise collection of the file data needed to *select* the malware detection processing method. The method in GB467 required the collection of the first portion of file data, the *implementation* of a first malware detection method to the first data, then, if necessary after obtaining the result from applying the first malware detection method, a second portion of file data could be collected and a second method of malware detection could be applied. This prior art method in GB467 requires the rigid sequential implementation of malware detection processing methods to the individual portions of file data obtained, if the results of the previous malware detection method warrant it.

22 It was argued by the agent for the applicant that the invention of the application in suit required the collection of the first file data and determining if a malware processing method *can be selected* from a plurality of malware detection processing methods based upon the first data and if not, obtaining second data relating to the selected file. The difference emphasised by the agent was that that the malware detection processing method was not implemented on the first data before collecting the second data; the first data was initially only used to determine if a malware detection processing method could be *selected.*

23 The second difference identified by the applicant was the use of the *combination of first and second data* to select a malware processing method if a malware detection processing method could not be selected using the first data alone. This appears in claim 1 in section (d) "*determining whether a malware detection processing method can be selected from the plurality of malware detection processing methods based upon* ***a combination of said first and second data***" (my emphasis added).

24 It was acknowledged in the hearing that the individual malware detection processing methods discussed in the application are all well-known and that the file data needed for each of the different malware detection processing methods are also well known.

25 Having considered the specification as filed and carefully considered the disclosure of GB467 in light of the applicants arguments as detailed in paragraphs 21-23 above, I am satisfied that the method disclosed in the application as filed:

(i) does not require the stepwise collection of file data to *select* a method of malware detection processing; and

(ii) does not require the *combination of first and second file data* to select a malware detection processing method.

Therefore, I consider that the invention as currently claimed in claim 1 of the application in suit is novel over GB467.

26 I note that no objection to the Inventive Step of the claims has been made during the processing of this application.

Support and Sufficiency

27 At the hearing the sufficiency of the disclosure as originally filed was discussed in detail. As already noted above, the applicant was also asked to provide further submissions to explain where, in the application as originally filed, the differences they identified between the application in suit and GB467 were set down. It was noted during the hearing that some embodiments described in the application as filed fall outside the claimed method, but that this was not unusual for a patent application during the amendment rounds. However, it was vital that the application as originally filed included at least one embodiment which disclosed the invention clearly enough and completely enough for the skilled person to put it into effect.

28 Having considered the written submissions provided by the applicant and reviewed the application as filed, I am satisfied that there is support in the description for the two differences between the invention as claimed and the prior art identified by the applicant. Thus, I consider that the requirement under section 14(5) of the Act has been met.

29 Turning now to the matter of sufficiency, Section 14(3) of the Act is intended to prevent a patentee laying claim to products or processes which the teaching of the patent does not enable the skilled addressee to perform. In *Eli Lilly v Human Genome Sciences*[2] at [239], Kitchin J gave the following summary of the relevant principles to be applied:

> *"The specification must disclose the invention clearly and completely enough for it to be performed by a person skilled in the art. The key elements of this requirement which bear on the present case are these:*
>
> *(i) the first step is to identify the invention and that is to be done by reading and construing the claims;*
>
> *(ii) in the case of a product claim that means making or otherwise obtaining the product;*
>
> *(iii) in the case of a process claim, it means working the process;*
>
> *(iv) the sufficiency of the disclosure must be assessed on the basis of the specification as a whole including the description and the claims;*
>
> *(v) the disclosure is aimed at the skilled person who may use his common general knowledge to supplement the information contained in the specification;*

[2] Eli Lilly v Human Genome Sciences [2008] RPC 29

(vi) the specification must be sufficient to allow the invention to be performed over the whole scope of the claim;

(vii) the specification must be sufficient to allow the invention to be so performed without undue burden."

30 When considering section 14(3), it is necessary to define the skilled person. There had been little or no discussion of who was the skilled person, or skilled team, during the processing of this application or at the hearing, however, in the subsequent written submission from the applicant, the agent, making particular reference to points (v) and (vii) above, stated that the skilled person was identified as "*being familiar with computer programming and would understand that malware detection processing methods are implemented in software as subroutines which take as their arguments input data associated with the file being scanned"* and that the skilled person *"would realise that the step of determining whether a malware detection method can be selected (from a plurality of available methods) and implemented by simply determining whether any of the subroutines/functions implementing these methods can be called using the obtained data*".

31 I fully agree with the applicants statements relating to the skilled person and so I have used them as a basis for defining the skilled person for this application. I consider that in this situation the skilled person would be a software engineer or computer programmer, familiar with all the malware detection processing methods which are commonly used and familiar with the file data necessary to input into the malware detection processing methods. They would also be aware of the relative processor power required to run the various malware detection processing methods and the relative ease of obtaining the different kinds of file data required for each malware detection processing method.

32 In the written submission following the hearing, the agent noted that the need for a sufficiency of the data is repeatedly mentioned in the application as filed, i.e., in **S5** of Figure 2, paragraph 2 of page 8 and paragraph 3 of page 9. However, at the hearing and in the written submission, it was acknowledged that the specification does not explicitly describe how to perform the assessment of whether the file data collected is sufficient to allow a malware detection method to be selected.

33 The applicant argued that, at the priority date, selecting which malware detection method to apply to a particular set of data would be known to a skilled person writing any computer program which uses the method. The applicant also argued that the skilled person would realise that the step of determining whether a malware detection method can be implemented could be done simply by determining whether any of the subroutines or functions implementing the malware detection processing methods can be called using the obtained data.

34 I agree that the skilled person would be able to determine which malware processing method *is suitable to* use on each individual portion of the file data collected, but this is different from determining that the file data collected so far *is sufficient* to allow a malware processing method *to be selected*.

35 One argument presented at the hearing was that the file data needed to select a malware detection processing method was not necessarily the same data as was

needed to input into the malware detection processing method. While this is an interesting point, it does not explain how the first data is used to select the malware detection processing method.

36 The first difference over the prior art presented at the hearing required that the first data collected "if sufficient" could be used to select the malware processing method and if a malware selection process could not be selected using the first data alone, then second data was obtained. There is no disclosure of how the first data is used to select or not to select a method of malware detection processing.

37 In my view the applicant was not able to identify a clear enough and complete enough disclosure in the specification as originally filed for the skilled person to be able to carry out this first identified difference. This step is a ***selection*** one – identifying the malware detection processing method that could be used - and not an ***implementation*** one - which involves actually running this malware detection processing method to find out what malware is present. Given the lack of information on how the first data is used to select rather than implement a malware detection processing method, I consider that his feature of the claimed invention is not disclosed in the specification as filed.

38 The second difference identified between the disclosure of GB467 and the claimed invention is determining whether "*a malware detection processing method can be selected from said plurality of malware detection processing methods based upon a combination of said first and second data and, if so, selecting a malware detection method"* as claimed in part (d) of claim 1. The application as filed is required to disclose in enough detail to enable the skilled person to select a malware detection method by combining the first and second data.

39 However, the application as filed only briefly refers to the combination of the first and second data (and perhaps also the third data and so on) in a few places (my emphasis added below as underline):

- in page 3 paragraph 2 which states that "*if the second data is insufficient to allow malware detection processing to be selected, third data relating to the selected file may be obtained to allow selection based upon the combination of the first, second and third data, and so on*";

- in page 9 paragraph 5 which states that "*if the data obtained…is together insufficient to allow malware detection processing to be selected ..[then]...data associated with a file type of the selected file is obtained*".

40 When discussing where and when the first and second data were combined and used for selecting the malware detection processing method, it was stated that this process would occur in the rules of the selection logic, depicted in block 11 of Figure 4; however this block has no written description associated with it. There are no other references to combining the first and second data than those mentioned above, no disclosure of how the data is combined, why the data is combined or how the combined data is used to select a single malware detection processing method.

41 A useful test for enablement was given in *Edison v Holland* [3]*,* which asks if anything new has to be found out by a person of competent skill following the directions in the specification in order to succeed; if the answer is yes, then disclosure in the specification is not complete enough.

42 The skilled man as described above, would not know how to "*determine whether a malware detection processing method can be selected from said plurality of malware detection processing methods based upon a combination of said first and second data".* Each malware detection processing method requires the input of specific file data. Simply combining the distinct types of file data, in an undisclosed way, to select a single malware detection processing method would require new information.

43 The above lack of disclosure of the required 'new information' also indicates that the disclosure is insufficient according to the classic statement of the test for insufficiency in *Valensi v British Radio Corporation*[4] which states:

> "*We think the effect of these cases as a whole is to show that the hypothetical addressee is not a person of exceptional skill and knowledge that he is not to be expected to exercise any invention nor any prolonged research, inquiry or experiment. He must, however, be prepared to display a reasonable degree of skill and common knowledge of the art in making trials and to correct obvious errors in the specification, if a means of correcting them can readily be found*."

Using the combined first and second data to select a malware detection processing method would, in my view, require "*invention or prolonged research, inquiry or experiment*". As noted in paragraphs 40 and 42 above there is no information on how to combine said first and second data to achieve the desired selection step. As set down in point (vii) of *Eli Lilly* (see paragraph 29 above), I consider that the specification is not sufficient to allow the invention to be performed without undue burden.

44 It is established practice that Section 14(3) of the Act means the applicant must ensure that, at the time of filing, the specification discloses the essential features of the invention in sufficient detail for the person skilled in the art to be able to put the invention into practice. If the disclosure of the invention claimed is not clear and complete enough, then either the application must be refused or the claims restricted to matter that is adequately disclosed. Any deficiencies in the specification cannot be rectified by adding technical matter after filing as this would contravene section 76 of the Act.

Other matters

45 At the hearing, there was some discussion as to whether claim 2 would be considered novel over the disclosure of GB467.

---

[3] *Edison & Swan Electric Light Co v Holland,* 6, RPC, 282, see page 282

[4] *Valensi & Anr v British Radio Corporation Ltd.* [1973] RPC 337, see page 377 (CA

46 As noted above, claim 1 has been found to be novel, thus it follows that claim 2, which is dependent upon claim 1, is also novel. Unfortunately, it also follows that, as the invention as claimed in claim 1 has been found not to be disclosed in the specification in a manner that is clear enough and complete enough for the invention to be performed by a person skilled in the art, any claim dependent upon current claim 1 will also suffer from this defect.

47 Additional features disclosed in the application or claimed in the dependent claims appear to be conventional.

Conclusion

48 Having considered all of the above, I find that the method of selecting a malware detection processing method claimed in claim 1 of the application in suit is novel over the disclosure in GB2463467A and, accordingly, does meet the requirements of section 1(1)(a) of the Act.

49 However, I find that the method of selecting a malware detection processing method as claimed in claim 1 is not disclosed in the specification as filed in a manner that is clear enough and complete enough for the invention to be performed by a person skilled in the art as required under section 14(3) of the Act.

50 After consideration of the application as originally filed, it is not readily apparent to me that this failure to meet the requirement under section 14(3) of the Act can be addressed by amendment. However, that is a matter that the applicant may want to consider.

51 I note that the prescribed period for putting this application in order expired on 28 December 2016 and that this period was extended, as-of-right, until 28 February 2017 under Rule 108(2) of the Patents Rules 2007, as amended (the Rules). I note that a further extension of this period under rule 108(3) of the Rules was requested by the applicant on 20 April 2017 while awaiting the outcome of the hearing and this decision (see letter from applicant dated 20 April 2017). This will bring the prescribed period for putting this application in order up to 28 April 2017. I consider that this request for an extension to the compliance date is acceptable

52 Should the applicant choose to file amendments, they would of course need to be searched and examined fully to ensure that they comply with the requirements of the Act.

53 If no amendments are received by the end of the prescribed period for putting this application in order, currently 28 April 2017, the application will be refused under section 18(3) of the Act for failure to comply with section 14(3) of the Act.

Appeal

54 Any appeal must be lodged within 28 days after the date of this decision.

Dr L CULLEN
Deputy Director, acting for the Comptroller