INTELLECTUAL
PROPERTY OFFICE

BL O/164/11

16 May 2011

PATENTS ACT 1977

APPLICANT	The Court of Edinburgh Napier University
ISSUE	Whether patent application number GB 1008261.8 complies with section 1(2)
HEARING OFFICER	B Micklewright

DECISION

Introduction

1 This decision concerns whether the invention claimed in patent application GB 1008261.8 relates to excluded subject matter.

2 International patent application PCT/GB2009/051142 was filed on 9 September 2009 in the name of The Court Of Edinburgh Napier University. The application had a declared priority date of 10 September 2008 and was published as WO 2010/029346 A1. It entered the GB national phase on 18 May 2010 and was allocated the GB application number GB 1008261.8 and subsequently republished as GB 2466908 A.

3 The examiner issued his first examination report on 5 July 2010 in which he argued that the invention disclosed in the application in suit was excluded from patentability as a program for a computer as such and a mathematical method as such. The applicant disagreed. After a further round of correspondence it became apparent that the examiner and the applicant were not going to reach agreement and the matter was therefore referred to me on 18 March 2011 for a decision based on the papers on the file.

The invention

4 The invention relates to carrying out digital forensic analysis of a digital computing system by collecting and analysing system call data (i.e. requests made between a user space and a kernel space) from the system so as to detect attack, intrusion or misuse of that system. The invention makes use of sequence matching techniques similar to those used in the bioinformatics field for protein

and DNA sequence matching analysis to detect matches between a test sequence of system calls stored in a database and a sequence derived from the collected system call data. In particular a gapped local biological sequencing algorithm is used to detect matches between test sequences of system calls and the sequences derived from the collected system call data. This analysis is used to determine whether certain events of interest have taken place so as to detect attack, intrusion or misuse of the system.

5 Claims 1, 16, 26 and 27 are all independent. Claims 1 and 16 are set out below. Claim 26 relates to a computer program that when executed enables the method of claim 1. Claim 27 relates to a computer program product comprising the computer program of claim 26 either recorded on a storage medium or available for download or other types of transmission. Claims 1 and 16 state:

> *1. A digital forensic analysis method comprising the steps of:*
>
> *collecting system call data from a digital computing system (DCS), said system call data comprising requests made between a user space and a kernel space of said DCS;*
>
> *converting the system call data to a sequence format;*
>
> *selecting from a system call sequence database a test sequence of system calls; and*
>
> *performing a sequence matching step using a gapped local biological sequence matching algorithm to detect matches between the test sequence of system calls and the sequence derived from the collected system call data.*
>
> *16. A digital forensic system comprising:*
>
> *data collection means for collecting system call data from a digital computing system (DCS) said system call data comprising requests made between a user space and a kernel space of said DCS;*
>
> *data formatting means arranged to convert the collected system call data to a sequence format; and*
>
> *sequence matching means arranged to apply a gapped local biological sequence matching algorithm to detect a match between said sequence derived from the collected system call data and a test sequence of system calls.*

The law

6 Section 1(1)(d) of the Patents Act 1977 (“the Act”) states that a patent may be granted only for an invention in respect of which the grant of a patent for it is not excluded by subsections (2) and (3) or section 4A. Section 1(2)(c) states that things which consist of “a scheme, rule or method for performing a mental act, playing a game or doing business, or a program for a computer” are not inventions for the purposes of the Act, but only to the extent that a patent or

application for a patent relates to that thing as such.

7 There is a large amount of case law in relation to these provisions. The most significant recent judgments of the Court of Appeal on the matter are *Aerotel Ltd v Telco Holdings Ltd Ors Rev 1* [2007] RPC 7 and *Symbian Ltd's Application* [2009] RPC 1. In *Aerotel* the Court of Appeal reviewed all the previous case law and specified the following four-step test as a methodology of determining whether an invention was excluded from patentability under section 1(1)(d):

> (1) Properly construe the claim;
>
> (2) identify the actual contribution;
>
> (3) ask whether it falls solely within the excluded subject matter;
>
> (4) check whether the actual of alleged contribution is actually technical in nature.

8 In *Symbian* the Court of Appeal confirmed that the above test is intended to be equivalent to the prior case law test of "technical contribution". In the present case I will therefore use the *Aerotel* test and ensure in my consideration of steps (3) and (4) that I determine whether the invention makes a technical contribution.

Assessment

(1) Properly construe the claim

9 The claims are in this case sufficiently clear and no construction issues arise. The applicant highlighted that the "system call data" comprises "requests made between a user space and a kernel space" and that the sequence matching algorithm claimed in the independent claims is, according to the claim, "gapped" and "local", which is evident from the wording of the claims.

(2) Identify the actual contribution

10 Although it seemed in the earlier correspondence that the examiner and the applicant disagreed on the identification of the actual contribution, there was not a great deal between them and both agreed that the actual contribution of claims 1, 16, 26 and 27 relates to a digital forensic analysis method and corresponding digital forensic system that provides for determining whether certain events of interest have taken place through the collection of system call data and the use of a gapped local biological sequence matching scheme.

11 The claims specify that system call data comprises requests between a user space and a kernel space but neither the claims nor the description provide a great amount of detail as to how this system call data is collected. I therefore conclude that the detail of how the system call data is collected is conventional and does not form part of the actual contribution.

12 In practice, according to the independent claims the use of a gapped local biological sequence matching scheme involves converting the data to sequence format, selecting a test sequence of calls, and then performing a sequence

matching step using the gapped local biological sequence matching algorithm.

(3) Ask whether it falls solely within the excluded subject matter

13 The applicant argued that the invention claimed in the present application is inherently a technical process that solves a technical problem. The contribution to the art is therefore of a technical nature. The various steps and features of the claim involve technical considerations. The applicant argued that the choice of the specific architectural point within the digital computer system's operating system at which to collect data is a technical consideration. The applicant also argued that the problem of how to sift through a morass of sequence call data and to provide intelligible identification of activities is inherently a technical one. The contribution lies in part with the collection of system call data from a digital computing system and this collection defines a technical process that is inherently not a mathematical method. Similarly the claim specifies a step of converting the system call data to a sequence format and again this is a technical transformation rather something that can be characterised as a mathematical method. In summary the applicant submits that, as a matter of practical reality, the means for specific events to be detected reliably in a digital forensic method provides a significant advance beyond mere sorting of data and provides a new capability and contribution that is inherently technical in nature. The invention does not give a contribution of being able to find data but instead makes a contribution that includes for the first time the collection of that data itself, rather than merely identifying patterns in it.

14 The examiner argued that the problem concerned data mining and referred to the Office decision in *Makor Issues and Rights Limited* (BL/O/181/07) in which the mathematical analysis of data using a computer program was found to be excluded as relating to a mathematical method and computer program as such. The applicant however argued that the new monitoring and forensic capabilities provided by the invention are more than simple data mining but are non-trivial engineering tasks. They distinguish their invention from that in *Makor Issues and Rights* by the process of collecting the system call data, which they say is not readily available or intelligible to a computer or to a machine, and then analysing it as defined in the other steps of the claim. This, they say, is entirely different from the mere data mining of sales data to which *Makor Issues and Rights* relates.

15 The applicant provided some examples of what may or may not be considered patentable. I did not find these examples particularly helpful in determining the present case. The examples were in the main hypothetical and the circumstances different from those of the application in suit. As the Court of Appeal said in *Symbian*, each case must be determined by reference to its particular facts and features, with reference to the relevant case law, and there is little to be gained in comparing the present case with largely hypothetical examples.

16 Whether or not the digital forensic analysis amounts to data mining, what it is doing is organising and analysing the collected data using mathematical techniques. The purpose, according to the application, is to identify suspicious patterns of activity. Moreover, according to the application the forensic analysis ultimately produces data for display to an operator assessing the activities taking

place on the digital computing system. There is no change to the performance of the computer or to a process external to the computer.

17 Taking all these matters into consideration I conclude that the digital forensic method and system relate to a program for a computer and a mathematical method as such. The system call data collection step is in itself conventional, the invention not lying in the way the data is collected but in the use of a particular matching algorithm to analyse the collected system call data. Using the particular algorithm defined in the claims for such a purpose may be new and may be effective but in substance it is merely a mathematical method implemented as a computer program and does not make any technical contribution which would take it outside of the excluded fields. There is no technical contribution either within or external to the digital computing system. I therefore conclude that the contribution lies entirely within the excluded subject matter.

(4) Check whether the actual of alleged contribution is actually technical in nature

18 In my analysis of step (3) above I have determined that the contribution is not technical in nature. The invention is therefore excluded from patentability as a program for a computer as such and a mathematical method as such.

Conclusion

19 I have found that the invention is excluded from patentability under section 1(2) of the Act as a program for a computer as such and a mathematical method as such. Moreover I have read through the application and cannot identify any amendment which would result in a patentable claim. I therefore refuse the application.

Appeal

20 Under the Practice Direction to Part 52 of the Civil Procedure Rules, any appeal must be lodged within 28 days.

B MICKLEWRIGHT
Deputy Director acting for the Comptroller