INTELLECTUAL PROPERTY OFFICE

BLO/174/09

23 June 2009

PATENTS ACT 1977

APPLICANT F-Secure Oyj.

ISSUE Whether patent application number GB 0604165.1 complies with sections 1(1)(b), 1(2)(c) and 14(5)(d)

HEARING OFFICER C L Davies

DECISION

1 This application was filed on 2nd March 2006 and was published under serial no. GB 2435700A on 5th September 2007.

2 Despite amendment of the claims during substantive examination, the applicant has been unable to persuade the examiner that the invention complies with sections 1(1)(b) or 14(5)(d) of the Patents Act 1977 (the Act) or that it is patentable within the meaning of section 1(2) of the Act. The matter came to a hearing before me on 26th February 2009 which was attended by Patent Attorneys Dr Robert Lind (who presented the applicant's arguments) and Dr Matthew Mitchell of Marks and Clerk and the Examiner Mr Nigel Hanley.

3 An offer of a hearing was originally made in an examination report issued on 12th May 2008. However, the agent took advantage of an as of right time extension and several discretionary extensions before reply on 27th November 2008. This allowed the Agent to frame his response in the light of the decision of the Court of Appeal in *Symbian's Application*[1].

4 Usefully, the examiner and the agent have discussed the case and agreed an approach that has led us to this hearing. Specifically, the examiner issued an Examination Report on 12th January which set out fully objections on the grounds of Inventive Step, Patentability and Plurality. The report also made it clear that the Examiner has not completed the examination for issues of clarity and support which will need to be addressed should I find in the applicants favour.

5 I am also grateful for the skeleton argument provided by Dr Mitchell before the hearing.

[1] Symbian's Application [2008] EWCA Civ 1066

The invention

6 The current set of claims on file were filed on 4th May 2007 and contains four independent claims which can be divided into two sets with claims 1-5 concerning a virus checking application and claims 6 & 9 a malware removal application. In each set at least one claim is directed to a method of executing the application and the other to a memory card containing the application on a memory card. There are also two omnibus claims, claims 7 & 8, to a method of executing an application and a memory card.

7 The method in both cases relies on a memory card being coupled to the mobile communications device and subsequently initiating the boot sequence on the device. Prior to completion of the boot sequence a "Symbian Recognizer" is loaded to the device from the memory card. This recognizer is then executed which in turn executes the virus checking or malware application which is also stored on the memory card.

8 The current claims read as follows:

Claim 1

A method for automatically executing an anti-virus application on a mobile communications device, the mobile communications device using a Symbian operating system, the method comprising;

coupling a memory card to the mobile communications device;

initiating a boot sequence on the mobile communications device;

prior to completion of the boot sequence, loading to the mobile communications device a Symbian recognizer from the memory card;

executing the loaded Symbian Recognizer on the mobile communications device to automatically execute the anti-virus application, the anti-virus application also being stored on the memory card.

Claim 3

A memory card for connecting to a mobile communications device, the memory card comprising data storage means having stored thereon:

an anti-virus application for executing on the mobile communications device;

a Symbian Recognizer component for automatically executing the anti-virus application when the memory card is coupled to the mobile communications device, prior to completion of a boot sequence of the mobile communications device.

Claim 6

A method for disabling malware on, or removing malware from, a mobile communications device, the method comprising;

coupling a memory card to the mobile communications device;

initiating a boot sequence on the mobile communications device;

prior to completion of the boot sequence, loading to the mobile communications device a Symbian recognizer from the memory card;

executing the Symbian recognizer on the mobile communications device, the Symbian recognizer being arranged to disable or remove the malware.

Claim 9

A method for disabling malware on, or removing malware from, a mobile communications device, substantially as described herein with reference to the accompanying drawings.

The relevant law

9 There are three issues to be decided. Firstly, I must decide if the application makes an inventive step. Secondly, I must decide if the application is for excluded matter and thirdly whether the application relates to more than one invention. It is therefore helpful if I set out the relevant law as it relates to each of these issues.

10 An invention shall be taken to involve an inventive step as required by section 1(1)(b) if, in accordance with section 3,

> "it is not obvious to a person skilled in the art, having regard to any matter which forms part of the state of the art by virtue only of section 2(2) above (and disregarding section 2(3) above)".

I do not think I need to quote sections 2(2) and 2(3), but it follows from these that the state of the art comprises all matter which has at any time before the priority date of the invention been made available to the public, whether in the UK or elsewhere.

11 Section 1(2) reads:

> "It is hereby declared that the following (among other things) are not inventions for the purposes of this Act, that is to say, anything which consists of –
>
> (a) a discovery, scientific theory or mathematical method;
> (b) a literary, dramatic, musical or artistic work or any other aesthetic creation whatsoever;
> (c) a scheme, rule or method for performing a mental act, playing a game or doing business, or a program for a computer;
> (d) the presentation of information;
>
> but the foregoing provision shall prevent anything from being treated as an invention for the purposes of this Act only to the extent that a patent or application for a patent relates to that thing as such.";

The examiner has raised objection under the computer program exclusion. I must interpret section 1(2) in accordance particularly with the decisions of the Court of

Appeal in *Symbian* and *Aerotel*[2], which I consider in detail below. It has been agreed by the both the Agents and the Examiner that this forms the correct basis for determining issues of excluded matter.

12 Section 14(5) reads:

> The claim or claims shall –
>
> (a) define the matter for which the applicant seeks protection;
> (b) be clear and concise;
> (c) be supported by the description; and
> (d) relate to one invention or to a group of inventions which are so linked as to form a single inventive concept.

Argument and analysis

Inventive step

13 The test for inventive step is the four-step *Windsurfing* test as reformulated by the Court of Appeal in *Pozzoli*[3]. I will now take each step in turn:

Identify (a) the notional person skilled in the art and (b) the relevant common general knowledge of that person

The examiner identified the skilled person as either a single person or a team of people who are used to programming mobile phones and also have an understanding of virus checkers. This view was shared by Dr Lind. I am also content with this identification of the skilled person.

The examiner identified that as part of their common general knowledge the skilled person would be well aware of the Symbian™ mobile phone Operating System given its market dominance and use in many mobile phones. As such, the use of recognizers as a means for loading applications is a known tool. They would also know that a valuable resource for any programmer, indeed any IT professional when faced with a problem would be the Internet and in particular technical fora where other users post their experiences and solutions. As such these would be regarded as a basic tool in the armory of the skilled person. The skilled person would also know that it is essential in virus protection to load a virus checker on a system as soon as possible to avoid the risk of infecting other machines.

Whilst this was generally accepted by the applicant, Dr Lind pointed out in both his skeleton argument and at the hearing that the use of recognizers was "expert knowledge" and not common general knowledge as asserted by the examiner. The application makes extensive use of a feature of the Symbian Operating System known as recognizers. The application on page 4 at Lines 17-19 provides an URL to the *Symbian Developers Technical Library*. Viewing this page on the

---

[2] *Aerotel Ltd v Telco Holdings Ltd* and *Macrossan's Application* [2006] EWCA Civ 1371
[3] See *Windsurfing International Ltd v Tabur Marine (Great Britain) Ltd* [1985] RPC 59 and *Pozzoli SPA v BDMO SA* [2007] EWCA Civ 588

Internet shows a copyright date of 2002. Dr Lind asserted that this specific reference forms “expert knowledge” and therefore not common general knowledge.

14 In considering this point, it is necessary for me to appreciate how recognizers work. It is clear from the *Developers Library* pages that recognizers run from a known directory on the system “*/system/recogs”* and that recognizers are interrogated to provide a link to data or applications. Furthermore, the applicant makes it clear in the specification that no amendment to the Symbian Operating System is required which implies to me that recognizers are standard features.

15 Following on from the above, I therefore take the view that recognizers form part of the common general knowledge of a skilled programmer. The date of the document itself would mean that the *Developers Library* has been known to the programmer for at least three years given the earliest date of the current application is 2nd March 2006. I would expect a skilled programmer to be aware that such a library existed given that it is a common feature of operating systems for such libraries to be made available to users. In my view it is the purpose of these libraries to make it easier for programmers to develop applications that run on these systems.

16 At the hearing, the discussion on the common general knowledge also raised an interesting issue on how the skilled programmer would use the Internet to search for a solution to a programming problem. The examiner has argued that when faced with a problem the skilled programmer would inherently look to the Internet for a solution. In particular, he would look to bulletin boards or specialist websites for a solution.

17 Dr Lind argued against this. If I can summarise, his point is that the skilled person would not look to the Internet unless they had identified a problem to solve and, specific to this case, had identified that they could use a Symbian recognizer to load a virus checking or malware removal application. Furthermore, he argues that the contents of Internet fora are “expert knowledge” and not common general knowledge.

18 As I have already said, I consider the use of recognizers to be part of the common general knowledge of the skilled person. Deciding whether the Internet fora form part of the common general knowledge is another point I need to determine.

19 Bulletin boards and the information contained within them is a result of the pooling of information from a number of contributors who are peers of the same skilled person/programmer and, for this reason, bulletin boards and their contents amount to knowledge which is shared between peers for the benefit of each other. To the skilled person, this is an important source of information. The key is the fact that they know where to look as much as to what the contents of the bulletin board are. Following from this, I believe that bulletin boards and their contents would form part of the common general knowledge of the skilled person/programmer and I do not accept that bulletin boards and their contents constitute only “expert knowledge”.

20 At this stage, I will also take the opportunity to establish how virus checkers are normally run and consider also whether this knowledge forms part of the common general knowledge. It is clear to me that it is well known to install and run a virus checker after a system has been booted. I believe it is also well known to execute a virus checker as part of the boot sequence as is common in the PC world. As I have said above the skilled person can be a team and in this case includes a person skilled in using virus checking software. I consider that their common general knowledge would include the knowledge of running a virus checker both as part of the boot sequence or after booting.

Identify the inventive concept of the claim in question or, if that cannot readily be done, construe it.

The examiner has identified the inventive concept as the running of a virus checker from a memory card attached to a mobile phone using a Symbian recognizer.

21 Dr Lind asserted in both his skeleton argument and at the hearing that there is an additional aspect to the inventive concept, namely "prior to completion of the boot sequence, loading to the mobile communication device a Symbian recognizer from the memory card."

22 Dr Lind outlined the problem identified by the applicant. He asserted that the inventor has recognized that, particularly in the case where the antivirus software is installed in a mobile shop or service centre, there is a high risk that viruses can be spread to other mobile devices whilst the device is operating and prior to execution of the anti-virus software. It will be appreciated that in a service centre, there may be tens or even hundreds of devices which could be infected, for example by a Bluetooth transmission, from the infected device. As this problem, namely the risk of infection for some (possibly short) period prior to installation of the anti-virus application, has not previously been recognized, the skilled person would not have thought to execute an anti-virus application from a memory card during the mobile device's boot sequence. Whilst it might have been obvious to install anti-virus software onto a mobile device from a memory card whilst the device is operating normally, and then to subsequently run the anti-virus software early in the boot sequence (i.e. when the device is subsequently switched off and rebooted), it would certainly not have been obvious to load and execute the anti-virus application from the memory card during the boot sequence.

23 I do not disagree with this and see the inventive concept of the claims as a method of invoking an application, namely a virus checker or malware removal program on a mobile communications device using a Symbian recognizer, with both the recognizer and virus checker/malware removal program located on a memory card which is inserted into the mobile device, the system then being initialized with the recognizer loading prior to completion of the boot sequence to execute the virus checker/malware removal program.

24 I would however, make one observation at this point. The specification makes it clear when talking about the cabir worm which spreads over the Bluetooth[RTM] protocol that in order for this to be spread the receiving user has to accept the file caribe.sis which contains the worm. Whilst I agree with the contribution as set out above I am not sure if the claimed invention actually offers a solution to the service centre problem as set out by Dr Lind – surely skilled individuals in a service centre would not accept a file as part of their standard operating procedures. This suggests to me that the applicant has developed a solution for something that, as a matter of practical reality, may not actually be the problem they envisage.

Identify what, if any, differences exist between the matter cited as forming part of the state of the art and the inventive concept of the claim or the claim as construed

25 On the basis of the prior art documents located by the examiner, he identified the difference between the inventive concept and the cited art to lie in the nature of the application program that is being run, ie. a virus checker or malware removal program. Dr Lind did not agree with this.

26 By disputing that recognizers and that use of the Internet to locate the SIEMENS and RAENTO documents (which do not solve the problem addressed by the applicant) do not form part of the skilled programmer's common general knowledge, Dr Lind asserted that one of the key differences between the present claim 1 and the cited prior art is that according to claim 1, the Symbian recognizer is loaded from the memory card prior to completion of the boot sequence.

27 Dr Lind asserted that the SIEMENS document was an odd starting point for determining the inventive concept, because it is an isolated thread on the Internet and also, since this thread has no relevance to anti-virus applications, it has no recognition of the problem being solved by the applicant.

28 I will now consider the prior art documents in some detail.

29 The cited prior art on this specification is found in the following documents and Patent Specifications:

SIEMENS	Siemens Community Forums: Autorun for an MMC card Slot Retrieved from http://agathonisi.erlm.siemens.de:8080/jive3/thread.jspa?threadID=15295
RAENTO	Symbian Programming – Starting applications automatically Retrieved from http:/web.archive.org/web/20041027013137/http://www.cs.helsinkii.fi/u/mraento/Symbian/autostart.html
NOKIA	WO 2006//038082
F SECURE	GB 2366693 A and GB 2378783 A.

30 The patent specifications are important to this case as they were responsible for the narrowing of the claims to their current form from those originally filed. To that extent they are instructive in assisting me in identifying the differences between the cited art and the inventive concept.

31 Both F-SECURE documents establish that it is known to run a virus checking application on a mobile communications device that uses the Symbian Operating System. The NOKIA document is perhaps more instructive as it shows clearly the loading of a virus checker application on a mobile communication device as part of a boot sequence. In common with the F-SECURE documents it too uses the Symbian Operating System.

32 The SIEMENS Internet citation is a community forum for programmers of the Symbian Operating System. The initial poster, “RobertG”, seeks help with the auto-running of an application from a memory card. The instructive post is the final post in which the poster “rorep” points to the RAENTO document and suggests the writing of an .mdl file which runs each time you insert the memory card or every time the phone is turned on.

33 The RAENTO document is found by following the hyperlink from the SIEMENS document. This document provides details on how you use a recognizer to start an application. RAENTO has realized that recognizers are loaded at start up and that you could embed code in one to start an application. RAENTO also notes that it is “sometimes not a good idea to start an application before the phone has booted completely since not all services are yet available”.

34 The RAENTO document also makes it clear that this in some instances may cause a problem with services not being available. However, in this instance I am not sure if this is actually a bad thing since if I understand the problem as set out by Dr Lind it is the very same services that may lead to the problem in the first place. For example without the loading of the Bluetooth^{RTM} wireless protocol a virus cannot spread via that method.

35 Taking the above prior art documents and what I have considered to be the common general knowledge into account, it is clear to me that the concept of using a Symbian recognizer to load an application as part of a boot sequence when both the recognizer and the application are on a memory card coupled to a mobile communications device, is not inventive. The fact that recognizers are loaded during the boot sequence suggests very strongly that they are loaded to and executed on the device prior to completion of the boot sequence. Returning to the claim, the only requirement is that the recognizer is loaded and executed prior to completion of the boot sequence. The claim only requires that the recognizer is executed during the boot sequence. It would appear that there is no requirement for the virus checker application to be executed during the boot sequence or that any executions finish before the boot sequence terminates.

36 The prior art is therefore considered to show that it is known to execute a Symbian recognizer from a memory card during the boot sequence of a mobile

communications device.

37 Following from the above and, like the examiner, I conclude that the only difference between the inventive concept and the cited prior art is the nature of the application itself that is being run. In the current case, the difference is whether the application being run is a virus checker, malware removal program or some other application (Claim 7).

Viewed without any knowledge of the alleged invention as claimed, do those differences constitute steps which would have been obvious to persons skilled in the art or do they require any degree of invention?

38 The examiner has argued that the skilled person would be aware that they can load an application using a recognizer from a memory card inserted into a phone prior to initiating a boot sequence. Given that the use of recognizers is to load and/or execute applications, the loading of a virus checker or malware removal program would appear to be an obvious step.

39 This leaves only the timing of the loading of the virus checker application. In my view, the skilled person would seek assistance from a person skilled in the art of loading and operating virus checkers. That person would know that it is imperative that a virus checker is loaded and executed at the earliest opportunity to avoid infecting other devices. As such, the timing would also appear to be obvious to the skilled person.

40 I therefore conclude that to use the method of executing a recognizer from a memory card during the boot sequence to launch a virus checking application would not require any inventive ingenuity on the part of the skilled person and find that the invention as set out in claims 1, 3 & 6 lacks an inventive step.

Dependent claims

41 The examiner has asserted that the dependent claims also lack an inventive step. I do not see the need to consider these in the same detail as above but I will deal with them in order.

42 Claim 2 is directed to initiating a boot sequence by powering on the system. Having found that claim 1 is not inventive, I can see nothing inventive in initiating a boot sequence by powering the device on. Indeed, this is perhaps one of the most common methods of initiating a boot sequence in computing.

43 Claim 4 is directed to the memory card having an installation means for installing the virus checking software. The use of installers is well known and for that reason I find that this claim also lacks an inventive step.

44 Claim 5 refers to the type of memory card. All the types listed in this claim are well known and the skilled programmer would require no inventive ingenuity in choosing or utilizing any of these cards. The card type would in any case be determined by the card that the mobile communications device can use. The SIEMENS document itself refers explicitly to the use of a CompactFlash^{RTM} card.

45 Claims 7-9 are omnibus claims. I have carefully read the specification and I cannot see any additional subject matter that could be covered by these claims that could make or contribute to an inventive step.

Excluded matter

46 During the examination of the case the Examiner has also argued that the invention is excluded under Section 1(2). I shall now address this issue.

47 In its recent decision in *Symbian* concerning the computer program exclusion the Court of Appeal approached the question of excluded matter primarily on the basis of whether there was a technical contribution. However the Court was quite clear (see paragraphs 8-15 of the decision) that the structured four-step approach to the question in its previous decision in *Aerotel* was never intended to be a new departure in domestic law; that it remained bound by its previous decisions, particularly *Merrill Lynch*[4] which rested on whether there was a technical contribution; and that any differences in the two approaches should affect neither the applicable principles nor the outcome in any particular case.

48 Indeed the Court at paragraph 59 considered its conclusion in the light of the *Aerotel* approach. I therefore consider it right to base my assessment of patentability in the present case on the same four-step approach as explained at paragraphs 40-48 of *Aerotel*, namely:

1) Properly construe the claim

2) Identify the actual contribution (although at the application stage this might have to be the alleged contribution); as explained at paragraph 43 this is "an exercise in judgment probably involving the problem said to be solved, how the invention works, what its advantages are"; it is essentially a matter of determining what it is the inventor has really added to human knowledge, and involves looking at substance, not form.

3) Ask whether it falls solely within the excluded matter, which (see paragraph 45) is merely an expression of the "as such" qualification of section 1(2).

4) If the third step has not covered it, check whether the actual or alleged contribution is actually technical.

49 The Court believed that it was possible, at least in principle, to reconcile this with the decision of the European Patent Office Board in *Duns Licensing Associates* (T 0154/04) criticising the *Aerotel* approach by conflating the third and fourth *Aerotel* steps. It was fortified in its view by the approach taken in a more recent decision of the Board in *Gameaccount Ltd* (T 1543/06) holding that patent protection should not be conferred "where the only identifiable contribution of the

[4] *Merrill Lynch's Application* [1989] RPC 561

claimed technical implementation to the state of the art is the excluded subject-matter itself". The Court stated at paragraph 15 that the *Gameaccount* approach:

> "…. plainly requires one to identify the contribution (which equates to stage 2 in *Aerotel*) in order to decide whether that contribution is solely "the excluded subject-matter itself" (equating to stage 3 in *Aerotel*), while emphasising that the contribution must be "technical" (effectively stage 4 in *Aerotel*). The order in which the stages are dealt with is different, but that should affect neither the applicable principles nor the outcome in any particular case."

Construction of the claims

50 This is not in issue and I do not in any case think that it presents any problems.

Identification of the contribution

51 The examiner's view is that the contribution lies in the nature of the application that is being executed. In his view the contribution can be viewed as the execution of either a virus checker or malware removal application on a mobile communications device. This is based upon the fact that the features leading to the execution of the application are all known and cannot therefore be part of "what the applicant has added to human knowledge" (*Aerotel paragraph 43*). Specifically, the examiner argues that the only contribution made is the choice of application being run given that it is known to use recognizers to launch an application.

52 Dr Lind for the applicant argues that this is too narrow a view and that the contribution lies in the arrangement of the virus checker being located on the memory card. Dr Lind went onto argue that this is potentially a better computing device in that it will reduce the risk of infections to other devices. He has also argued that the use of the memory card is akin to a new arrangement of equipment as in *Aerotel*.

53 I have already discussed at some length the prior art and the common general knowledge. As I see it, the fundamental issue to be decided in determining the contribution is whether the contribution includes executing the application from the memory card during the boot sequence or is it merely the nature of the application being run?

54 There can be little doubt that running an application from a memory card cannot be part of the contribution – this seems to me (acknowledged by Dr Lind also), to be a standard way to install software onto a mobile communications device. In fact, I would go as far to say that loading software from a storage device is ubiquitous in the world of computing.

55 The key to the contribution as defined by Dr Lind is therefore the timing of the loading. This comes back to the service centre problem identified by Dr Lind which is essentially the practical application of the method of the invention. In this environment you firmly close "the window of opportunity" for infection by inserting

the memory card into a mobile phone/communications device before you turn it on. Once you turn it on, thus initiating the boot sequence, the virus checker is automatically loaded and executed. The result of this is that you are now safe in the knowledge that you have not infected any other phones in the service centre.

56 The contribution as seen by the applicant is reliant on the feature of using a recognizer to load and execute the application. However, it is acknowledged in the specification that no changes need to be made to the Symbian Operating System to invoke the loading and execution of the virus checker. It follows from this that recognizers are standard components of the operating system and their main purpose is to launch a further program component. It is also known that these recognizers run during the boot sequence.

57 In the light of this I therefore consider that in this instance the contribution lies in the nature of the application being run and the time at which it is run. More specifically, the contribution is in the use of a known utility, i.e. a recognizer, which is installed to the device in a completely standard mode and is used to call an application which happens to be a known virus checker.

Does the contribution fall solely within excluded matter or does it make a "Technical Contribution"?

58 In my view the identified contribution is inherently a computer program when viewed in its most narrow sense and by a strict application of the four step test of *Aerotel* would appear to be excluded. However, following the decision in *Symbian* I must also consider whether it makes a "technical contribution" and if I find it does then it is allowable and not excluded by virtue of Section 1(2)(c) of the Act.

59 Technical contribution or as it has sometimes been referred to "relevant technical effect" has been notoriously difficult to define. In *Symbian,* Neuberger LJ states that:

> "it would be dangerous to suggest that there is a clear rule available to determine whether or not a program is excluded".

He then went on to say that:

> "it must mean, consistently with *Vicom* and the two *IBM Corp* cases, that a technical innovation, whether within (as in the last mentioned cases) or outside the computer will normally suffice to ensure patentability".

60 I believe it is important to look at the application in the light of the problems it seeks to solve both internally and externally to the communications device. Internally, the virus checker is being loaded as part of the boot sequence which in itself is not particularly innovative. However, using this method does close the "window of opportunity" for the device to infect other devices thus solving the external problem.

61 The claimed invention is clearly implemented using computer programs. In fact, the programs used are in reality nothing more than a variant of known programs

in the case of the virus checker and of a known utility in the use of a recognizer. For this reason I do not see how the use of these programs can be considered to form part of a technical contribution or technical innovation to use Neuberger LJ's words – they may be technical and require a technical understanding of their function but they do not provide a technical contribution or any technical innovation to this application.

62 The question I am left with therefore is "Does the timing of the execution provide a technical contribution?" Here again I do not think it does. The applicant has made it clear that no amendment is required to the operating system and it is clear from the references he provides in the specification that it is known for recognizers to operate as part of the boot sequence. It follows that the use of recognizer in this manner cannot contribute to a technical contribution as it is already a well known feature.

63 This leaves only the nature of the application being run – the virus checker or the malware removal tool. It appears that this is little more than a choice of program for execution by the recognizer that is being made.

64 Following from *Symbian*, I must also consider whether I am left with a better machine. The application is a method of executing a virus checker on a computing device as a result of the use of known programming arrangements. This appears to me to be a better programming technique rather than a better machine. I believe therefore that I am not left with a better machine.

65 For the above reasons I consider the invention to be also excluded from patentability as a computer program under Section 1(2)(c) of the Act.

Plurality of Invention

66 The objection on the grounds of plurality of invention has come about as a result of the amendment of claims to overcome the original novelty objection and the examiner's view that the common subject matter between the claims is known. At the hearing Dr Lind sought to dispense with this objection by removing claims 6 and 9 from the application.

Conclusion

67 I therefore conclude that the invention of claims 1-9 is excluded under section 1(1)(b) as the claims do not make an inventive step. I conclude also that the invention is excluded as a computer program under section 1(2)(c). Having read the specification I have been unable to identify any amendments which would avoid exclusion under either section 1(1)(b) or 1(2)(c). I therefore refuse the application under section 18(3).

Appeal

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

C L Davies
Deputy Director acting for the Comptroller