Intellectual Property Office

BL O/353/16

25 July 2016

PATENTS ACT 1977

APPLICANT	Lionel Wolovitz
ISSUE	Whether patent application GB1405450.6 complies with section 1(2)
HEARING OFFICER	J E Porter

DECISION

Introduction

1 Patent application GB1405450.6 entitled "Methods and apparatus for brokering a transaction" results from the entry into the UK national phase of international patent application PCT/GB2012/052337 in the name of Lionel Wolovitz. The international application was filed on 21 September 2012, with an earliest declared priority date of 28 September 2011. It was published as WO 2013/045898 on 4 April 2013, and was reprinted as GB 2 508 776 A after entering the UK national phase.

2 Following a number of rounds of correspondence between the examiner and the applicant's attorneys, and amendment of the claims, the examiner remains of the view that the claimed invention is excluded from patentability under section 1(2).

3 With the position unresolved the applicant asked to be heard and the matter came before me at a hearing on 6 April 2016. Dr Wolovitz attended the hearing and was also represented by his patent attorney Mr Nick Bebbington of Beck Greener. The examiner Ms Sally Vinall and an observer Ms Becky Lander were also present and I was assisted by Dr Sarah Whitehead of Patents Legal Section.

The invention

4 The invention is concerned with a system and method for brokering a transaction between a first party and a second party by use of a trusted transaction server (TTS). The transaction being brokered may in principle be any type of transaction and may include actions such as making a payment, withdrawal of money from an ATM, logging in to an online service, or other transactions between parties. The system is arranged such that the two parties do not share sensitive information with each other via a non-secure channel, such as the internet. Instead each party is authenticated with the TTS via a trusted communication channel, and only a non-sensitive transaction code is passed directly between the parties via the non-secure channel. The TTS receives the transaction code and brokers the transaction by

requesting transaction details and supplying relevant information to the party responsible for approving the transaction.

5 The latest amended claims were filed on 30 March 2016, a week before the hearing. However, these claims simply contained minor changes to the pre-existing claim set (filed on 7 December 2015), with the intention of addressing clarity issues raised by the examiner in her communication of 3 February 2016. The substantive matter before me remains that identified in relation to the previous claim set, and it does not turn on these clarity points.

6 A set of auxiliary claims was also filed on 30 March 2016, with the request that I consider these claims, should I find that the claims on file relate to unpatentable subject matter.

7 In terms of the claims now on file, there are 62 claims of which 6 are independent. Claims 1 is a claim to a system and reads as follows:

> *A system for brokering a transaction between a first party and a second party, the system comprising:*
>
> *a Trusted Transaction Server (TTS);*
>
> *a first application running on a first computing device connected to the TTS by a first, trusted communication channel; and,*
>
> *a second application running on a mobile computing device connected to the TTS by a second, trusted communication channel,*
>
> *the first application being arranged to send a request for a brokered transaction from the first party to the TTS over the first communication channel, the request comprising at least some transaction details;*
>
> *in response to receiving said request, the TTS being arranged to authenticate the identity of the first party and store at least some transaction details received from the first party together with a transaction code;*
>
> *the first application being arranged to communicate the transaction code to the second party;*
>
> *the second application being arranged to receive an input of the transaction code from the second party by manual input or by scanning a machine readable code and being arranged to send a message to the TTS over the second communication channel containing the transaction code;*
>
> *in response to receiving the transaction code from the second application, the TTS being arranged to match the transaction code received from the second party with the transaction details for that transaction code stored at the TTS and to send a request for authorisation for brokering the transaction from the TTS to the second party including at least some of the details of the transaction for display on the mobile computing device,*
>
> *the second application being arranged to receive a secret code entered by the second party on the mobile computing device and authorisation for the transaction to be brokered and to send a message to the TTS authorising the transaction to be brokered,*
>
> *the TTS authenticating the identity of the second party by way of the secret code and brokering the transaction with the first party and/or a third party including sending information necessary for authorisation of the transaction to the first party and/or third party.*

8 Independent claim 2 is also directed to a system and reads:

> *A system for brokering a transaction between a first party and a second party, the system comprising:*
>
> *a Trusted Transaction Server (TTS);*
>
> *a first application running on a first computing device connected to the TTS by a first, trusted communication channel; and,*
>
> *a second application running on a mobile computing device connected to the TTS by a second, trusted communication channel,*
>
> *the first application being arranged communicate a transaction code to the second party;*
>
> *the second application arranged to receive an input of the transaction code from the second party by manual input or by scanning a machine readable code and being arranged to send to the TTS over the second communication channel a request for a brokered transaction from the second party including the transaction code containing information identifying the first party and the transaction,*
>
> *in response to receiving the request, the TTS being arranged to match the first party with first party details stored at the TTS using the information identifying the first party contained in the transaction code, the details including details of communications with the first party,*
>
> *the TTS being arranged to authenticate the first party and establish a first communications channel between the TTS and the first party based on the details, and then to send the transaction code from the TTS to the first party over the first communication channel;*
>
> *the first application being arranged to send to the TTS over the first communications channel from the first party at least some transaction details;*
>
> *the TTS being arranges to store the transaction code received from the second party with at least some details of the transaction received from the first party and to send a request for authorisation for brokering the transaction from the TTS to the second party including at least some of the details of the transaction for display on the mobile computing device,*
>
> *the second application being arranged to receive a secret code entered by the second party on the mobile computing device and authorisation for the transaction to be brokered and to send a message to the TTS authorising the transaction to be brokered,*
>
> *the TTS authenticating the identity of the second party by way of the secret code and brokering the transaction with the first party and/or a third party including sending information necessary for authorisation of the transaction to the first party and/or third party.*

9 Independent claims 31 and 32 are method claims directed to methods of brokering a transaction in almost identical terms to the systems set out in claims 1 and 2 respectively.

10 Independent claim 61 is directed to a TTS constructed and arranged to carry out the method for brokering a transaction of the preceding claims and independent claim 62 is directed to a computer program containing instructions for causing a computer to carry out the method performed by the second application of any claim.

11 The attorney agreed at the hearing that the independent claims would stand or fall together on the issue before me.

The law

12 Section 1(2) declares that certain things are not inventions for the purposes of the Act, as follows:

> *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.*

13 The examiner and the applicant agree that the assessment of patentability under section 1(2) is governed by the judgment of the Court of Appeal in *Aerotel*[1], as further interpreted by the Court of Appeal in *Symbian*[2].

14 In *Aerotel*, the court reviewed the case law on the interpretation of section 1(2) and approved a four-step test for the assessment of what is often called "excluded matter", as follows:

> *Step one: properly construe the claim*
>
> *Step two: identify the actual contribution (although at the application stage this might have to be the alleged contribution)*
>
> *Step three: ask whether it falls solely within the excluded matter*
>
> *Step four: check whether the actual or alleged contribution is actually technical in nature.*

15 Subsequently, the Court of Appeal in *Symbian* made clear that the *Aerotel* test is not intended to provide a departure from the previous requirement set out in case law, namely that the invention must provide a "technical contribution" if it is not to fall within excluded matter. The *Aerotel* test has subsequently been endorsed by the Court of Appeal in its decisions in both *HTC*[3] and *Lantana*[4].

16 Lewison J (as he then was) in *AT&T/CVON*[5] set out five signposts that he considered to be helpful when considering whether a computer program makes a

---

[1] *Aerotel Ltd v Telco Holdings Ltd and Macrossan's Application* [2006] EWCA Civ 1371, [2007] RPC 7

[2] *Symbian Ltd's Application* [2008] EWCA Civ 1066, [2009] RPC 1

[3] *HTC Europe Co Ltd v Apple Inc* [2013] RPC 30

[4] *Lantana Limited and The Comptroller General of Patents, Designs and Trade Marks* [2014] EWCA Civ 1463

[5] *AT&T Knowledge Venture/CVON Innovations v Comptroller General of Patents* [2009] EWHC 343 (Pat)

technical contribution. In *HTC* the signposts were reformulated slightly in light of the decision in *Gemstar*[6]. The signposts are:

> *i) Whether the claimed technical effect has a technical effect on a process which is carried on outside the computer.*
>
> *ii) Whether the claimed technical effect operates at the level of the architecture of the computer; that is to say whether the effect is produced irrespective of the data being processed or the applications being run.*
>
> *iii) Whether the claimed technical effect results in the computer being made to operate in a new way.*
>
> *iv) Whether the program makes the computer a better computer in the sense of running more efficiently and effectively as a computer.*
>
> *v) Whether the perceived problem is overcome by the claimed invention as opposed to merely being circumvented.*

17 The attorney's submissions in response to the examination reports, in his skeleton argument and at the hearing covered various points concerning how the *Aerotel* test should be applied to the claimed invention in question and the relevance of the *AT&T/CVON* signposts. I consider these submissions as part of my analysis below.

Arguments and analysis

18 The examiner maintains that the claims define an invention which consists of a program for a computer and a method for doing business. Her position is set out most recently in her letter of 3 February 2016. Detailed arguments against the examiner's position are contained in the applicant's responses to the examination reports, through his attorney, but in particular are set out in the skeleton argument provided on 30 March 2016. These arguments were elaborated clearly and helpfully at the hearing, both by Mr Bebbington and by Dr Wolovitz. Taking all these arguments into account, I must determine whether the claimed invention relates solely to excluded subject matter under section 1(2).

Properly construing the claims

19 Throughout the examination process, the examiner and the attorney have been in agreement that (minor clarity issues notwithstanding) the scope of the claims is sufficiently clear that there have been no issues arising under step one. Nevertheless there were a number of points of construction on which further clarification was provided at the hearing.

20 Independent claims 1 and 2 both relate to a system for brokering a transaction, and Mr Bebbington and Dr Wolovitz explained that the two claims differ only in the ordering of the steps by which the transaction code is generated. I also noted that these claims are defined in terms of components which are “arranged to" do a particular action. Mr Bebbington explained that the intention is to capture the way in which the applications within the system configure the network links to create the

[6] *Gemstar-TV Guide International Inc v Virgin Media Ltd* [2010] RPC 10

secure path. I agree that the claims as drafted bring out not just the various components listed but also that these components perform the tasks required.

21 Mr Bebbington and Dr Wolovitz were keen to emphasise that the invention is applicable across a wide range of potential applications and that terms such as "brokering" and "transaction" should not be interpreted as meaning that the invention is limited to financial or business transactions. From their submissions and the range of embodiments given in the description, I agree with their point. “Brokering” is taken to refer to the request and supply of information to give rise to an action being taken by a remote computer; “transaction” is construed to include a wide range of actions done via a computer network, such as logging in to a website.

22 There is a small outstanding drafting point regarding claim 2, with the claim having an initial reference to a “first, trusted communications channel” and then subsequent references to “a first communications channel”. Mr Bebbington confirmed at the hearing that these were one and the same feature.

23 Therefore, claims 1 and 2 concern a system for brokering a transaction between two parties, comprising a TTS, a first application running on a computer and a second application running on a mobile computing device. Each application is connected to the TTS via its own trusted communication channel. In response to a request, the TTS authenticates the identity of the first party and stores transaction details. A transaction code is communicated from the first application to the second party, and is input into the second application by the second party. The claims are limited such that the second application is arranged to receive the input of the transaction code by manual input or by scanning a machine readable code. A message containing the code is then sent to the TTS. The TTS uses the transaction code to identify relevant transaction details, which are stored at the TTS along with the transaction code. The TTS then sends an authorisation request to the second party, which includes at least some of the transaction details. The second party authorises the brokering of the transaction by input of a secret code into the second application, and a message is sent to the TTS authorising the transaction. The TTS thus authenticates the identity of the second party, and it then brokers the transaction with the first party or a third party, sending any necessary information to them.

24 As already noted, I am content that independent claims 31 and 32 are construed as claims directed to methods of brokering a transaction which correspond to the systems set out in claims 1 and 2 respectively.

25 Independent claim 61 is directed to a TTS constructed and arranged to carry out the method steps required for brokering a transaction as set out in the preceding claims. Independent claim 62 is directed to a computer program containing instructions for causing a computer to carry out the method performed by the second application of any claim. As clarified at the hearing, this is therefore a claim to the application installed on the second party’s mobile computing device and which carries out the steps performed by the "second application" in preceding method claims.

Identifying the actual or alleged contribution

26 In paragraph 43 of *Aerotel*, it is made clear that identifying the contribution is probably best summed up as determining what the inventor has really added to

human knowledge, and this involves looking at the substance and not the form of the claim (as construed in step one). However, the court in *Aerotel* acknowledged that, for a patent application (as opposed to a granted patent), it may only be possible to identify the alleged, and not the actual, contribution. That must particularly be the case in such applications as the present one, where no search has been completed.

27 The examiner does not consider that the contribution lies in a new arrangement of hardware, nor in elements of the invention performing in a new or non-conventional way. Her position is that it is well known to connect mobile devices or merchant systems to a TTS via a secure channel. The examiner also says that the prior art shows that it is well known to transfer information between systems or applications by manual input or QR code. She argues that the elements of the invention are all used in a standard way from a technical viewpoint, and so the contribution must lie in the use of conventional hardware, connected conventionally, to exchange data in a particular way – such that sensitive data is shared only with the TTS. Her view of the contribution is then set out on pages 2 and 3 of the pre-hearing report.

28 The examiner goes on to acknowledge the advantage provided by the invention is that "the customer (or second party) does not need to provide any information to the merchant (or first party), or vice versa, since the parties can share a common transaction code over a non-secure communication channel and individually provide that code to the TTS to allow the TTS to match the authentication with the transaction request and broker that transaction".

29 At the hearing we explored the working of the various elements of the system. Mr Bebbington and Dr Wolovitz were clear that the individual hardware components are themselves entirely conventional, and that having secure or encrypted communication channels is well-known. Neither was there any suggestion that assigning a transaction code to each particular transaction, or manually inputting or scanning a code, are in themselves features which are considered new.

30 However, the attorney is critical of the extent to which the examiner then relies on the assertion that various elements of the invention perform in known or conventional ways. Mr Bebbington submits that it is necessary to consider what contribution is made by the system as a whole, as well as the individual elements, as made clear in *Aerotel*. I agree that this approach is correct. Where a particular aspect of a system is known, it does not necessarily follow that any contribution made by that aspect can be dismissed. What is required is to assess the contribution made by the claimed invention as a whole, and so the interaction between the various aspects (known or otherwise) needs to be considered when making that assessment.

31 The attorney submits that the contribution lies in establishing an "air gap" between the secure connections, and between the first and second applications. Only the transaction code is passed over the air gap between the first and second parties. He argues that the transaction code thus allows both applications to form trusted channels to the TTS and to “triangulate” the connections. This enables a transaction to be brokered securely without the need for sensitive data to be passed through a non-secure connection between the two parties involved.

32 The attorney argues that the architecture of the system is therefore different from prior art systems, as it uses a different arrangement of communication links between

the parties. For example, as neatly demonstrated at the hearing, the transaction code can be transmitted from one party to another via a web browser and then input manually or via a machine readable code into an app on a mobile device. The code allows the TTS to "tie together" the secure communication channels by which the transaction details are transmitted, and authentication with the TTS is achieved. Thus at the hearing both Mr Bebbington and Dr Wolovitz argued that the system is "architecturally new" and that it provides a new effect by way of using the passing of a transaction code over an air gap to give a secure end-to-end trusted connection between the parties, thus allowing a transaction to be brokered in a secure way.

33 One question is whether there is a new combination or arrangement of hardware in the sense that one was found to exist in *Aerotel*. In that judgment, the system as a whole was (at that point, although matters changed during later litigation) held to be new, and the contribution made was held (at para 53) to be a new system since "the key to it is a new physical combination of hardware".

34 In correspondence before the hearing, there had been some discussion about whether elements of the present invention were arranged or interacting in the same way as certain pieces of prior art that had been chosen as examples by the examiner. It seems to me that Mr Bebbington was not in the end attempting to go as far as saying that the invention was a new physical arrangement of hardware. At the hearing he said this: "In the *Aerotel* decision we're talking about a new combination of hardware elements into a new system. We're not quite saying in this case the hardware elements are new or assembled in a new way. What we're saying is there are technical real-world features, which arise through this system and the scheme it implements, which are new".

35 At the hearing I asked Mr Bebbington and Dr Wolovitz to expand on why they saw the contribution as being a new system architecture if the hardware and networks used were conventional, and the hardware elements were not assembled or physically combined in a new way. Dr Wolovitz explained that the various pieces of hardware would need to be configured to operate in the required way, and that this involved installing the application or an Application Programming Interface (API) on the relevant devices and/or websites, and developing the TTS and integrating the parties' system so that they could communicate securely with it.

36 Mr Bebbington expanded on his submission saying that the new technical architecture really comes apparent during operation. New paths are created via the sequence of communications over individual secure links and the air gap – and that is where the new architecture comes about. He argued that the contribution is therefore a "new combination of technical features" which brings about a more secure system overall. This has the advantage that the passing of sensitive information over non-secure channels is avoided. Thus, for example, if there was malware or key-logging software on a user's computer, it would only capture the transaction code, and not passwords or other sensitive data. So the problem solved by the invention is accessing, logging into or otherwise interacting with a remote computer via an unsecured network.

37 Weighing all this up, I think it is clear that the devices are not combined, arranged or networked to each other in new physical ways. Each device or application communicates securely with the TTS in a known way, and the devices and

applications of the first and second party are not connected to each other in a new way or via new means.

38 Furthermore, I do not see that there is anything added to the sum of human knowledge in terms of the manner in which the elements of the system interact with each other. Paths are created and then choices made about which of certain information or data is exchanged down those paths, in such a way which makes it more difficult for a hacker or malware to obtain sensitive or personal information. But the conventional elements and networks of the system are not in themselves more secure or interacting in a new manner. Where the skeleton argument refers to "establishing a trusted path over the channel in a novel way", it was clarified at the hearing that it is the steps leading up to the establishing of the path which are said to be novel, not the technical details of the trusted path itself. As the attorney made clear at the hearing, he is not saying that any individual network link is more secure than in the prior art. Thus in my view, whether it is a device communicating with the TTS via a secure channel, the transaction code being transferred from the first application to the second party's device, or the inputting of that code via manual or scanned input, these interactions and links are not ones which have been added to the sum of human knowledge by the present invention.

39 In my view, this points away from characterising the contribution as wide as a new approach to transaction of secure data. It seems to me that the contribution is contained in the steps that are taken to establish paths whereby particular information is exchanged in a particular order and a particular way. In my view, the contribution made by the invention is that it creates connections and supplies certain information across secure and non-secure communications channels in a particular order, such that sensitive information is provided, and authentication is performed, across secure communication channels between the first and second parties and the TTS. The transaction code is used to join secure connections at the TTS, by providing information from one network to the other, in the form of a unique identifier which allows information relating to the transaction to be correlated.

40 It is worth making a further point about the various embodiments which relate to use of the invention in different transactions. These include financial transactions, controlling ATMs, logging in to secure websites, and controlling a user's access to a locked area – where the lock is controlled by a remote computer linked to the TTS and the user has a mobile device. My assessment of the contribution does not turn on the particular application of the invention to any one of these embodiments, and it is independent of the particular data being transacted (whether financial, personal or otherwise). Clearly, it is also the case that using the program in relation to particular hardware devices (e.g. an ATM, a lock) does not make the contribution any wider than I have already identified.

Does the contribution fall solely within excluded matter / is it technical in nature?

41 What I must now decide is whether the contribution identified above relates solely to a program for a computer or a scheme, rule or method for doing business. This corresponds to step three of the *Aerotel* test. The fourth step of the test is to check whether the contribution is technical in nature. In paragraph 46 of *Aerotel* it is stated that applying this fourth step may not be necessary because the third step should have covered the question. This is because a contribution which consists solely of

excluded matter will not count as being a "technical contribution" and will not, as the fourth step puts it, be "technical in nature". Similarly a contribution which consists of more than excluded matter will be a "technical contribution" and so will be "technical in nature". In this case, the arguments concerning whether the invention is excluded are very much wrapped up with the question of whether the contribution is technical in nature. Given that, I have considered the third and fourth steps together.

42 The examiner's contention is that the contribution is a computer program and also a business method. She says that contribution is not technical, since any technical aspects of the invention are conventional. There is no new arrangement of hardware, there is nothing technical in the exchange of particular transaction information between the relevant parties, nor in the means of authentication of each of the parties to the TTS, nor the transaction code. She asserts that the business context of the invention is inherent to the invention and that, without it, the characteristic features of the claims cannot be provided. The attorney and the applicant put forward a number of reasons why they believe this view is wrong.

43 One is that the transaction code has technical functionality in that it allows the TTS to link together the two trusted channels by “triangulating” the first and second applications via the TTS. Thus, they say, the transaction code “comprises technical information” rather than information with any business-related meaning, and it is in essence being used to set up a new network.

44 Furthermore, they argue that the problem being solved is a technical one – that is to say – the problem of malware, hacking and general interception of data over the internet. It is a “fundamental technical problem” that the internet is not secure, and it is that to which the invention is directed. Network security is, they argue, a technical problem where there are practical real-world effects. The real-world effect of the invention is that hackers cannot compromise the system. This is, they say, an effect outside of the computer or network.

45 Thus they contend that the difference that the invention makes is that the transaction between the parties is set up so that sensitive data is kept secure, and the user does not have to identify themselves by inputting personal details in a non-secure way. That is the difference, as a matter of practical reality, even though the underlying hardware is the same as known hardware in the way in which it makes the necessary connections.

46 There was brief discussion of the *AT&T/CVON* signposts, which Mr Bebbington rightly identified as useful indicators as to where previous computer implemented inventions may have had a technical effect. His view was that they do not apply well to an invention concerning networked computers, and are more geared to a single computer running a program. His point here was that the technical effect is in the network and so it is not necessarily meaningful to talk about a technical effect being internal or external to a computer. In terms of whether the invention is excluded as a program for a computer, he focussed on the fifth signpost, and his position was that the invention was not circumventing a network security problem, but solving the problem of transacting with or controlling a remote computer over a non-secure network by making it possible to do this more securely.

47 Mr Bebbington also drew an analogy with the internet in general, arguing that the invention of the protocols which divide up information into packets and route it around networked computers using IP addresses would have been regarded as technical (and solving, not circumventing, a problem), even though networked computers were already known and the internet was using those existing links.

48 My view of these various points is as follows. First, I am not convinced by the argument that the transaction code is technical of itself. It is clear that it is used to identify the transaction so that the parties can transact in the way claimed. While it must follow that the connections are then made between the parties, I do not see that the fact that the network connections are then made in a particular arrangement bestows on the code a technical aspect. Although the attorney referred to the code as "triangulating", I could not see that this amounted to more than ensuring that the correct linkages and channels of communication were made between the correct parties and the TTS. Indeed, at the hearing the attorney explained that the transaction code "can be a random stream of digits" which "really just identifies the particular session or transaction we're concerned with".

49 On the question of what problem the invention solves, and what it contributes as matter of practical reality, it is important to bear in mind that the attorney's points were to an extent based on arguments that the contribution was wider than I have found to be the case. Had I agreed (for example) that the contribution made by the invention was a more secure network, then the consideration of whether such a contribution was a technical one would be different from the one I must carry out. But the contribution is the narrower one that I have identified. It follows that I agree with the examiner that any improvement in network security arises from the way in which the invention shares particular information via the channels and with the particular parties, and ensures that certain information is not sent through a non-secure channel. For this reason, I do not see that the improvement in security arises from a contribution which makes improvements of a technical nature. It is a contribution concerning choices about the order in which particular information is routed and exchanged around secure and non-secure channels.

50 This also relates to the attorney's point about the fifth *AT&T/CVON* signpost. As is clear from my reasoning, I am not convinced that the contribution made by the invention has solved a technical problem with secure or non-secure internet connections, and transactions made over them. It circumvents the issues that exist when transactions are carried out over non-secure connections, by ordering the passing of information via particular secure or non-secure routes, rather than solving technical problems with those non-secure connections.

51 In terms of the other signposts, I think the attorney was right that they do not assist greatly in this case. Nevertheless, for completeness: for the above reasons I do not detect a technical effect on a process carried on outside the computer (or network), and I agree there is no suggestion that the claimed technical effect operates at the level of computer architecture (in terms of the way a computer runs), or makes the computer operate in a new way, or more efficiently or effectively as a computer.

52 Finally, the analogy that Mr Bebbington made with the invention of the internet was interesting, but I am sure there are considerable dangers in relying on analogies, and in speculating on whether a claim to the internet would or would not have been

allowable at a particular time. I am on much safer ground if I determine the question before me by applying the law specifically to the facts of this case.

53 I am therefore not convinced that the contribution made by the invention is a technical one, or that it extends beyond being more than a program for a computer as such. As a result, it fails to comply with steps three and four of the *Aerotel* test and so the invention falls solely within excluded matter.

54 As noted above, the examiner raised an objection that the invention was also excluded as being no more than a scheme, rule or method for doing business. In my view, a contribution which amounted solely to the software identifying users with a particular transaction and exchanging particular information would be likely to be regarded as one that was purely administrative in nature, and so within the business method exclusion. However, since the contribution made by the software is that it establishes paths whereby the information is exchanged in a particular order and a particular way, I find that – on balance – this takes it beyond a pure administrative step, and so the invention does not amount to a scheme, rule or method for doing business.

The alternative claim set

55 The alternative claims are limited to using the system for secure signing in to a computer system. Mr Bebbington explained that the intention is to focus the claims on the technical field of accessing computer systems, in case the main claims failed because they encompassed within their scope financial transactions. In the event, the main claims fail not because of the nature of the transactions or the type of data they encompass. The contribution I have identified and assessed is independent of a particular transaction or data, and includes within its scope the secure sign-in embodiment. It follows that limiting the claims to secure sign-in to a computer system as the particular transaction does not change my assessment, and so the alternative claims must fail for the same reasons as the main claims.

Conclusion

56 I conclude that the claimed invention is excluded from patentability under section 1(2)(c) because it is no more than a program for a computer.

57 Based on the information before me, I cannot identify material in the specification that could reasonably be expected to form the basis of a patentable claim. I refuse the application under section 18(3) for failure to comply with section 1(2)(c).

Appeal

58 Any appeal must be lodged within 28 days

Dr J E PORTER
Deputy Director acting for the Comptroller