Intellectual Property Office

BL O/701/21

24 September 2021

PATENTS ACT 1977

PARTIES	Lookout, Inc.
ISSUE	Whether patent application GB1511914.2 complies with Section 1(2) of the Patents Act 1977
HEARING OFFICER	Ben Buchanan

DECISION

Background

1 This decision relates to whether patent application GB1511914.2 complies with section 1(2) of the Patents Act 1977 ("the Act").

2 The application is the national phase of a PCT application filed on 28 October 2013 and published as GB2523710A. The PCT application was originally published as WO 2014/105263 A1 and has an earliest priority date of 28 December 2012.

3 The initial rounds of examination and amendment were directed at resolving significant issues regarding the inventiveness and clarity of the claims and have been very helpfully summarised by the examiner in his report of 17 June 2021. Once the clarity issue was addressed to the extent that the examiner considered that the claims could be satisfactorily construed, he issued an examination report on 17 March 2021 objecting, inter alia, that the invention was excluded from patentability by virtue of section 1(2) of the Act. In his examination report of 28 April 2021 the examiner identified the state of the art and did not object to the inventiveness of the claims. In that and the final examination report, the only substantive objection raised was to patentability under section 1(2).

4 Despite further amendment and argument on behalf of the applicant, the examiner has maintained his objection that the application is excluded, all other remaining issues having apparently been resolved to his satisfaction. The applicant requested to be heard on the matter in their letter of 27 May, but that request was subsequently withdrawn in favour of a decision based on the papers on file.

5 The only matter which falls to be decided here is whether or not the invention is excluded under section 1(2)(c) as being a program for a computer and/or a method for doing business as such.

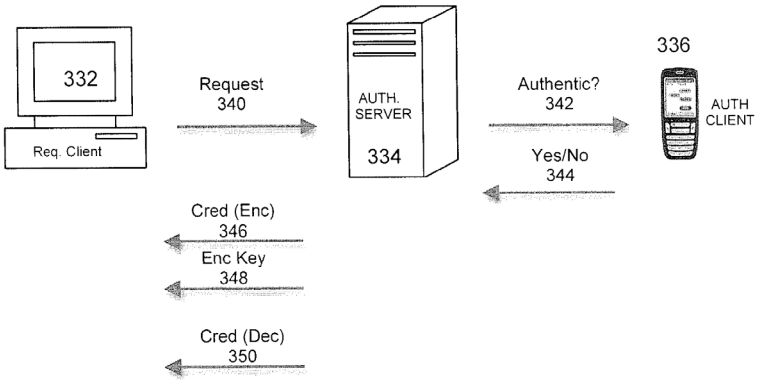
Subject matter

6 The application as a whole covers various methods for improving authentication of a user of a client computer to allow access to a network resource via a server. In particular, it covers techniques for providing multi-factor authentication, i.e. authentication methods which combine multiple different methods for identifying a user of a client computer. Furthermore, the techniques are intended to be relatively simple for widespread application using an authentication device that is readily available to most users. In contrast, the application claims that biometric methods, e.g. using fingerprints, can add considerable cost and complexity. Examples of the methods for identifying a user covered by the application include username and password combinations, context information, such as location and usage patterns of the client computer, and use of separate devices, e.g. a mobile phone associated with the user, in conjunction with a computer

7 Throughout the application process, the terms “authentication” and “authorisation” have both been used. In construing the claims, in particular in his examination report of 10 February 2021, the examiner queried the clarity of the claims in this respect. In response, accompanying their letter of 2 March 2021, the applicant amended the claims to define authorisation. I think this is a very helpful distinction and it now forms the basis for the claimed invention. The claimed inventive concept is not in verifying a user is who say they say they are (although that *authentication* step occurs in the claim); rather it is in ensuring a user is *authorised* (by a second, authorising user) to access a network resource via a server.

8 The particular method now claimed requires a first credential such as a combination of a username and password and, if the username and password are successfully verified, authorisation by a separate authorising person. More specifically, the server sends a request for authorisation to an authorising device associated with the authorising person and only allows access to the requested resource if valid second credentials are entered into the device by the authorising person; i.e. if the authoring person is *authenticated*.

9 The general arrangement is shown in figure 3b of the application (reproduced below) and reference should also be made to paragraphs [0095] and [0162] of the application. In the context of parents authorising access for children, paragraph [0172] is relevant.



The law

10 The examiner raised an objection under section 1(2)(c) of the Act that the invention is not patentable because it relates to one or more categories of excluded matter. The relevant provisions of this section of the Act are shown below:

> *1(2) 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*
>
> *…*
>
> *(c) a scheme, rule, or method for performing a mental act, playing a game or doing business, or a program for a computer;*
>
> *…*
>
> *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.*

11 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]. In *Aerotel* the court reviewed the case law on the interpretation of section 1(2) and set out a four-step test to decide whether a claimed invention is patentable:

> *(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 or alleged contribution is actually technical in nature.*

12 The Court of Appeal in *Symbian* made it clear that the four-step test in *Aerotel* was not intended to be a new departure in domestic law; it was confirmed that the test is consistent with the previous requirement set out in case law that the invention must provide a "technical contribution". Paragraph 46 of *Aerotel* states that applying the fourth step of the test may not be necessary because the third step should have covered the question of whether the contribution is technical in nature. It was further confirmed in *Symbian* that the question of whether the invention makes a technical contribution can take place at step 3 or 4.

13 Lewison J (as he then was) in *AT&T/CVON*[3] set out five signposts that he considered to be helpful when considering whether a computer program makes a technical

---

[1] *Aerotel Ltd v Telco Holdings Ltd & Ors Rev 1* [2007] RPC 7
[2] *Symbian Ltd v Comptroller General of Patents* [2009] RPC 1
[3] *AT&T Knowledge Ventures/CVON Innovations v Comptroller General of Patents* [2009] EWHC 343 (Pat)

contribution. In *HTC/Apple*[4] the signposts were reformulated slightly in light of the decision in *Gemstar*[5]. 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.*

Application of the *Aerotel* approach

Step (1): Properly construe the claim

14 The latest claims are the amended claims filed on 27 May 2021. There are two independent claims; claim 1 to a system, and claim 8 to a method, for authorising a user of a client computer. There are no substantive differences between the claims and they can be treated as sharing the same inventive concept. I will therefore consider only claim 1, and my finding in respect of patentability will apply by extension to claim 8. Amended claim 1 reads as follows:

> *1. A system for authorising a user of a client computer making a request to access a network resource, the system comprising:*
>
> *a client computer arranged to receive the request from the user to access the network resource and first credential information of the user and send a first request for authorisation of the user and the first credential information to an authorising server;*
>
> *wherein the authorising server:*
>
> *receives the first request for authorisation of the user and the first credential information from the client computer,*
>
> *verifies the user using the first credential information,*
>
> *determines, in response to verification being successful, using the first credential information, an authorising user that is different from the user,*

[4] *HTC v Apple* [2013] EWCA Civ 451
[5] *Gemstar-TV Guide International Inc v Virgin Media Ltd* [2010] RPC 10

determines, based on the determined authorising user, an authorising device that is associated with the authorising user and is different from the client computer, and

sends a second request for authorisation of the user to the authorising device, the second request requesting second credential information as authorisation; and

wherein the authorising device receives the second request and, in response thereto, prompts the authorising user to provide the second credential information to the authorization server as authorisation, wherein:

upon, the authorising user providing the second credential information and receipt of the second credential information from the authorising device, the authorising server verifies the second credential information and, in response to verification being successful, provides an authorisation of the user to the client computer, and, upon receipt of the authorisation of the user, the client computer allows the user to access the network resource.

15 Although the examiner has set out his construction of the claims based on claim 8, it is equally applicable to claim 1. The examiner makes the following comments in relation to his construction of the claim:

- 'Authorising person' is used in place of 'authorising user' to minimise the risk of confusion with the 'user'. The user and authorising person are taken to be natural persons.
- Claims 1 and 8 specify first/second credentials which are verified. This is taken to mean authentication of the user's identity/role (i.e. proving who they are).
- For clarity an access right linking the user, the network resource and the authorising person is included. The claims, not unreasonably, assume the case where there is an access right and it does involve an authorising person.
- It is taken to be the case that non-responses will likely be interpreted by the authorising server as rejections, thus a response from the authoriser is only essential for approvals.

16 I agree with the substance of the construction adopted by the examiner which is as follows:

An access control method wherein

a) A user inputs a request to access a first network resource and a credential into a client computer;

b) The client computer sends a message requesting access to the first network resource and the credential to an authorising server;

c) The authorising server verifies/authenticates the user using the credential;

d) If the user is verified determining the user's access rights;

e) If the user has a right to access the first resource subject to approval by an authorising person, determining the identity of the authorising person and of a device associated with the authorising person by which they may be contacted;

f) The authorising server sends a message to the determined contact device requesting that the authorising person approve/reject the resource access request;

g) The authorising person approves/rejects the request and provides an authentication credential (at least for approvals);

h) The contact device sends a response message to the authorising server (at least for approvals);

i) The authorising server verifies/authenticates the authorising person using the credential (at least for approvals);

j) If the request is approved and the authorising person authenticated, the authorising server sends a message authorising/enabling access to the first network resource to the client computer.

Step (2): Identify the actual or alleged contribution

17 Guidance on how to identify the contribution is given in paragraph 43 of *Aerotel*, where the court accepted the proposition that identifying the contribution is:

> *"an exercise in judgment probably involving the problem said to be solved, how the invention works, what its advantages are. What has the inventor really added to human knowledge perhaps best sums up the exercise. The formulation involves looking at substance not form."*

18 Identifying the contribution is not the same as determining the inventive step. Nonetheless the examiner's analysis of the state of the art, and the applicant's explanation of the key features of the invention provide some helpful context. These are set out in various correspondence, in particular the examiner's report of 17 June 2021 and the applicant's letter of 16 April 2021. The latter refers to a previous version of the claims, but the subsequent amendments are limited to clarification of the authorising user. The arguments in this letter appear to have persuaded the examiner that the latest claims are inventive.

19 To my mind, the problem is how to *independently* verify authorisation of a first user. That is to say, enable verification that authorisation is provided, independently of a first user and their computer (to reduce the likelihood of fraudulent authorisation). The claimed invention works by verifying a first user's identity, and dependent thereupon, identifying a different second user who must authorise the first user's access to a

requested resource. The invention sends an authorisation request to a *different, separate* device associated with the authorising user. By implication, the device is uniquely associated with the authorising user. The authorising user is verified using the separate associated device and (upon successful verification) provides authorisation for the first user to access the requested resource. The advantage is that this two factor authentication enables authorisation for user access independently of the first user computer, and additionally requires a second user to be verified using a separate device before authorisation is confirmed.

20 This goes somewhat further than the examiner's summary that the contribution is to an administrative policy including an "ask a human" step. For example, the invention specifically precludes a second, authorising user entering the requested second credentials on the first user computer. Likewise, the request for authentication is sent to a device which cannot be selected by the first user (for example by entering a mobile telephone number or directing a web browser).

21 It seems to me that the claimed invention and the contribution include essential elements ensuring the independence of the second user authorisation, by using a second authorising device associated with the second user and separate authentication of the second user.

22 In the correspondence on file, I respectfully consider that neither the examiner nor the applicant have satisfactorily identified the contribution. The applicant has repeated the entirety of claim 1, albeit with the second half of the claim relating to the authorising person being highlighted. On the other hand the contribution identified by the examiner is very brief and does not specify the elements I have identified above. However, they both have in common that the important part is the authorisation by the authorising person.

23 I consider the contribution to be as follows:

> Access control in which an access request made by a verified user is authorised by a second authorising user, the identity of the authorising user and a device associated with that user being determined by an authorising server, the authorising server sending a request for authorisation to the device and the authorising person responding with a credential, verified by the authorising server, to provide the authorisation.

<u>Steps (3) & (4): Does the contribution fall solely within the excluded subject matter; check if the contribution is actually technical.</u>

24 The third and fourth steps of the *Aerotel* test involve considering whether the contribution falls solely within excluded categories, and then checking whether the contribution is technical in nature. It is appropriate to consider these two steps together because whether the contribution is technical in nature will have a direct impact on whether it falls solely within excluded matter.

25 Although the contribution is implemented using a computer program running on a network of computers, that does not mean that it should immediately be excluded as a computer program as such. In *Symbian*, the Court of Appeal stated that a computer program may not be excluded if it makes a technical contribution.

26 In order to determine if the contribution is technical in nature I will consider the *AT&T* signposts.

27 For reasons which will become apparent I will start by considering the second to fourth signposts, the so-called *better computer* signposts.

Second signpost - 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

28 It is clear the effect of the invention does not operate at the level of the architecture of the computer in the sense of the operation of the processor, memory, or other internal components. The contribution specifically relates to a computer program for authorising user access to a restricted resource. The effect is therefore clearly dependent on the data being processed. The applicant has not made any argument to the contrary. The second signpost does not assist the applicant.

Third signpost - whether the claimed technical effect results in the computer being made to operate in a new way

29 In relation to the third signpost the applicant argues that because the invention is novel and inventive it must be operating in a new way. However, this signpost requires that the computer must "in general" operate in a new way, not merely that it should perform some specific new function. If that were not the case then substantially all computer programs would result in computers operating in some specific new way rendering the exclusion meaningless. The computer of the invention does not operate in a new way, it merely runs new application software, and this signpost does not point to the application being technical.

Fourth signpost - whether the program makes the computer a better computer in the sense of running more efficiently and effectively as a computer

30 Similarly, the applicant argues that signpost (iv) is also met as the invention provides a new and improved authorisation system which operates in a more efficient and effective way. Yet the authorisation is performed only by specific software running on the computer, and any improvement in the authorisation system is only due to an improvement in the software. The computer itself does not run more efficiently or more effectively. Accordingly this signpost also provides no assistance to the applicant.

First signpost – whether the claimed technical effect has a technical effect on a process which is carried on outside the computer

Fifth signpost - whether the perceived problem is overcome by the claimed invention as opposed to merely being circumvented

31 Having dealt with the second, third and fourth signposts I will consider the first and fifth.

32 The applicant identifies three ways in which they argue that there is a technical effect outside the computer.

33 Firstly, they argue that the client computer goes from a state of not being able to access the network resource to the state of being able to access it. Secondly, they suggest that the user goes from a state of not being able to access the network resource to the state of being able to access it. However, the examiner argues that in neither of these cases is there any effect on a process outside of the computer (as a network). I agree. Furthermore, the limitation of not being able to access one part of the network and the removal of that limitation is implemented within the software of the computer network. There are no hardware changes involved, for example.

34 Thirdly, they point to the fact that multiple physical devices are used to achieve the required user authorisation in order to enable the user of the client computer to access the network resource. In response the examiner has suggested that this argument is unrelated to the issue of whether or not there is an effect outside the computer and instead appears to be directed to an argument that the arrangement corresponds to a new arrangement of hardware. The examiner asserts that the arrangement is "entirely normal", although none of the prior art is referenced to demonstrate this (examination report of 17 June 2021, para.40).

35 Of these positions, I find the applicant's third closest to my own, with the clarification that authorisation is provided by a second user, using second authentication credentials, by using a separate second, authorising, device associated with the second user.

36 It is important to define what is meant by "the computer" in respect of this signpost. As the examiner points out in their report of 17 June, in *Lantana*[6], the Court directed that the "computer" may be a system of computers; a network computer. In so far as the user client computer, the network resource server and the authorisation server are concerned, I agree. Those devices are connected together to control and enable access to the requested resource. The authorising device is separate; deliberately independent even. I am not inclined to consider it as unitary with the "network computer". The process of interaction between the computer and the authorising device would therefore be outside the computer and the resultant effect is one of verification and authorisation to access the network resource. I regard access-control / security as a technical field of endeavour and on that basis would regard the effect of the contribution to mean that the first signpost is met.

37 If I am wrong on this definition of "the computer", then I consider that the independent second user interaction with the authorising device is outside the computer as a whole, in enabling access for the first user, in dependence upon "the computer" as a whole. That too would seem to satisfy the first signpost. It is an "improved" access control system wherein an authenticated second user controls a first user's access to a secure resource, using a computer. Put simply, in terms used by the examiner, this is not "ask a parent"; but is "ask a parent and ensure the parent independently authorises the request on a separate, authenticated device".

38 I therefore find that the contribution involves a technical effect outside the computer sufficient to satisfy the first signpost.

---

[6] Lantana v Comptroller-General of Patents [2013] EWHC 2673 (Pat)

39 Equally, I consider this to be a solution to the problem of providing independent authorisation for a user to access a system. Is that a technical problem? In as much as it concerns controlling access to a secure resource using a physically independent device, yes I believe it is. As such it is also considered to meet the fifth signpost.

40 In view of the fact that both the first and fifth signposts point to the contribution being technical, I consider that the contribution is technical in nature and the invention does not solely consist of a program for a computer as such.

41 In reaching this decision I note also the decision of the High Court in *PKTWO*[7]. *PKTWO* involved the generation of an alert message automatically sent from a computer to a remote terminal monitored by a supervisor, e.g. a text message to a mobile phone, alerting the supervisor to the fact that inappropriate content was being accessed on the computer. Floyd J found that the contribution was technical, in part because he considered the alert to be a physical concept rather than an abstract one, and it was akin to the *Transfer Patent* of *Gemstar*.

42 A similar consideration appears to apply to the instant case whereby the authorisation request notification delivered to an authorising person's device is physical rather than abstract such that there is a technical effect. The analogy, insofar as it holds, would appear to support my reasoning.

43 I have referred once or twice in this decision to the inventiveness of the claimed invention. Inventive step and excluded matter are separate considerations and are not necessarily inter-dependent. However, from what I can gather from the file, it is the sequence of steps, in particular the independent second authorisation step that has persuaded the examiner of the inventive step (which was not objected to after his report of 17 March 2021). His argument against patentability under section 1(2) seems predicated on the apparatus and *authentication* features being common general knowledge per se, thus he alleges the claimed invention, implemented by a computer program, consists of an (inventive) administrative or security policy. I agree it is a fine line, however, as I have explained above, I consider the claimed arrangement and operation of the hardware to be essential for the identified contribution. Unlike in an assessment of inventive step, where what is known is stripped away from the claimed invention to identify the difference, it can still form an essential contextual component of the contribution for assessing excluded matter and that is the case here. As a consequence, when put into effect, I consider the invention to be more than an administrative policy, or a method for doing business as such.

44 I therefore find that the claimed invention satisfies the requirements of section 1(2).

Conclusion

45 I find that the claimed invention provides a technical contribution and does not define subject matter excluded from patentability by section 1(2). Consequently I remit the application to the examiner for final preparations to ensure compliance with section 18(3) and grant.

---

[7] *Protecting Kids the World Over (PKTWO) Ltd's Application* [2011] EWHC 2720 (Pat)

46 Although the extended compliance period ended on 28th August, a further extension will be agreed should it be required to complete preparations for grant.

Appeal

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

Ben Buchanan
Deputy Director, acting for the Comptroller