Intellectual Property Office

BL O/611/19

09 October 2019

PATENTS ACT 1977

APPLICANT	Google LLC
ISSUE	Whether patent application GB 1715687.8 complies with sections 1(1)(b) and 1(2)
HEARING OFFICER	Dr C. L. Davies

DECISION

Introduction

1 Patent application GB 1715687.8 ("the application") entitled "Identifying consumers in a transaction via facial recognition" was filed on 28 April 2016, with an earliest declared priority date of 30 April 2015. It was published as GB 2552119 A on 10 January 2018.

2 Prior to substantive examination taking place, the claims were amended in line with the granted claims of the US equivalent, US 9619803 B2. However, following a number of rounds of correspondence between the examiner and the applicant's attorneys, the examiner remains of the view that the claimed invention is excluded from patentability under section 1(2); does not involve an inventive step; and is insufficient by excessive claim breadth. Whilst the examiner has deferred full substantive examination, including updating of the search, at this stage, she has raised a minor clarity issue which remains outstanding.

3 With the position unresolved the applicant asked to be heard. The issues before me were set out in the examiner's pre-hearing report of 10 January 2019. Upon consideration of the pre-hearing report prior to the hearing I decided it would be more efficient to split the issues to be heard. The issue of insufficiency by excessive claim breadth led to two lines of argument for excluded matter i.e. one for the current broader claim and one narrower claim overcoming the insufficiency issue. This along with the possibility of any amendment to overcome the insufficiency objection having an effect on the excluded matter and inventive step objections led me to consider deciding on the issue of insufficiency only in the first instance to be the most efficient approach. Therefore, following consultation with the applicant's attorney, it was decided that at the initial hearing on 1 April 2019 I would hear argument relating to the issue of insufficiency by excessive claim breadth only. My decision was issued as BL O/325/19 on 7 July 2019 and found in favour of the applicant that the claims are sufficient.

4 This left the issues of excluded matter and inventive step to be decided and the matter came before me at a hearing conducted via video conference on 18 July 2019. The remaining issues before me were set out in the examiner's updated pre-hearing report of 17 June 2019. The applicant was represented at the hearing by attorney Mr Mike Williams of Marks & Clerk LLP. The examiner Ms Becky Lander was present and I was assisted by Mr Marc Collins.

The invention

5 The invention relates to identifying a user at a particular location. In the application the invention is described in an embodiment concerning a transaction between a customer (user) and a merchant. Figure 1 is reproduced below. A merchant and a user 101 register with a payment processing system 160, which establishes a facial template based on a user image. The user signs into a payment application via a user computing device 110, which receives an identifier from a merchant beacon device 120 to transmit to the payment processing system. The payment processing system transmits facial templates to the merchant camera device 140 for other users who are also signed in to the payment application in range of the merchant beacon device. The merchant camera device compares a captured facial image against the received facial templates to identify the user. A merchant POS device operator 102 selects an account of the user. The merchant POS device 130 transmits transaction details to the payment processing system, which processes the transaction with an issuer system. The payment processing system receives an approval of the transaction authorization request and transmits a receipt to the merchant POS device.

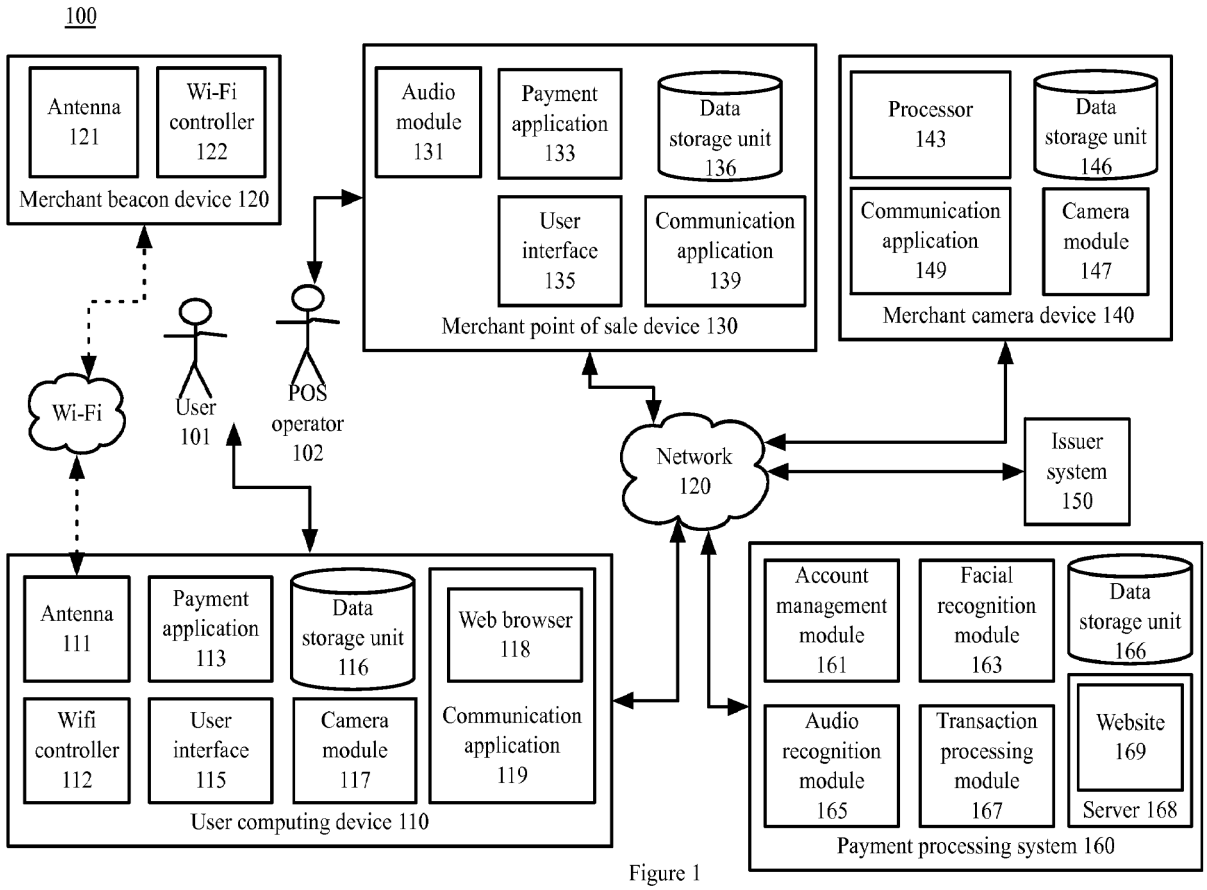

Figure 1

6 At the hearing Mr Williams explained that the invention is entirely concerned with how to perform automatic identification of a user at a location. In particular, it is concerned with how to do this in manner that does not require the user to provide some kind of documentary evidence or to manually engage in providing for example biometrics like fingerprints. In general, there are security concerns when dealing with the identification of users. The invention seeks to provide hands-free identification whilst providing security features and privacy benefits at the same time.

7 The latest set of claims filed on 18 October 2017 has twenty claims including four independent claims – claims 1, 7, 12 and 17. The independent claims are set out below:

> *1. A computer-implemented method to identify users at locations by comparing facial imaging of users against facial templates of users known to be at particular locations, comprising:*
>
> *broadcasting, by a computing device, an identifier associated with the computing device at a location;*
>
> *receiving, by the computing device and from one or more other computing devices, one or more facial templates, each facial template associated with a corresponding user associated with a corresponding user computing device that received the broadcasted identifier at the location and retransmitted the identifier to the one or more other computing devices, each facial template comprising a representation of a respective facial image of the respective user;*
>
> *storing, by the computing device, the one or more received facial templates;*
>
> *capturing, by a camera module of the computing device, a video feed of an environment external to the computing device;*
>
> *extracting, by the computing device, a facial image of a particular user from the video feed;*
>
> *generating, by the computing device, a facial template of the particular user based on the facial image of the particular user, wherein the facial template of the particular user is a representation of the facial image of the particular user;*
>
> *determining, by the computing device, a similarity between the generated facial template of the particular user and each of the one or more stored facial templates;*
>
> *identifying, by the computing device, a particular stored facial template as corresponding to the generated facial template of the particular user based on the determined similarity between the generated facial template of the particular user and the particular stored facial template exceeding a threshold value indicating that the stored facial template corresponds to the generated facial template of the particular user;*
>
> *transmitting, by the computing device, a response to a request to identify a user comprising an indication of the identified particular user.*
>
> *7. A computer-implemented method to identify users at locations by comparing facial imaging of users against facial templates of users known to be at particular locations, comprising:*

receiving, by one or more computing devices and from a particular user computing device, an account identifier of an account associated with a particular user associated with the particular user computing device and a beacon device identifier, wherein the particular user computing device retransmits the beacon device identifier received via a network from a beacon device at a location associated with the beacon device identifier;

retrieving, by the one or more computing devices, a facial template associated with the account of the particular user based on the account identifier of the account associated with the particular user;

identifying, by the one or more computing devices, the location associated with the beacon device identifier;

adding, by the one or more computing devices, the facial template associated with the account of the particular user and the associated location to a current customer log comprising facial templates corresponding to user computing devices that retransmit the beacon device identifier received from the beacon device at the location associated with the beacon device identifier;

transmitting, by the one or more computing devices and to a computing device at the location, the current customer log comprising the facial template associated with the account of the particular user, wherein the computing device identifies the particular user based on identifying the facial template associated with the account of the particular user from the current customer log as being similar to a facial template of the particular user generated from a facial image of the particular user captured by the computing device.

12. A computer program product, comprising:

a non-transitory computer-readable medium having computer-readable program instructions embodied thereon that when executed by a computer cause the computer to identify users at locations by comparing facial imaging of users against facial templates of users known to be at particular locations, the computer-readable program instructions comprising:

computer-readable program instructions to broadcast an identifier associated with the computing device at a location;

computer-readable program instructions to receive, from one or more computing devices, one or more facial templates, each facial template associated with a user associated with a user computing device that receives the broadcasted identifier at the location and retransmits the identifier to the one or more computing devices, each facial template comprising a representation of a respective facial image of the respective user;

computer-readable program instructions to store the one or more received facial templates;

computer-readable program instructions to receive a request to identify a user;

computer-readable program instructions to capture, by a camera module, a video feed of an environment external to the computer;

computer-readable program instructions to extract a facial image of a particular user from the video feed;

computer-readable program instructions to generate a facial template of the particular user based on the facial image, wherein the facial template of the particular user is a representation of the facial image of the particular user;

computer-readable program instructions to retrieve the one or more stored facial templates associated with one or more corresponding user computing devices that retransmitted the identifier broadcasted at the location;

computer-readable program instructions to determine a similarity between the generated facial template of the particular user and each of the one or more stored facial templates;

computer-readable program instructions to identify a particular stored facial template as corresponding to the generated facial template of the particular user based on the similarity between the generated facial template of the particular user and the particular stored facial template exceeding a threshold; and

computer-readable program instructions to transmit a response to the request to identify the user comprising an indication of an identity of the particular user.

17. A system to identify users at locations by comparing facial imaging of users against facial templates of users known to be at particular locations, comprising:

a storage device; and

a processor communicatively coupled to the storage device, wherein the processor executes application code instructions that are stored in the storage device to cause the system to:

receive, from a particular user computing device, an account identifier of an account of a particular user associated with the particular user computing device and a beacon device identifier, wherein the particular user computing device retransmits the beacon device identifier received via a network connection from a beacon device at a location associated with the beacon device identifier;

retrieve a facial template associated with the account of the particular user based on the account identifier of the account of the particular user;

identify the location based on the beacon device identifier;

add the facial template associated with the account of the particular user and associated location to a current customer log comprising facial templates corresponding to user computing devices that retransmit the beacon device identifier received via the network connection from the beacon device at the location associated with the beacon device identifier; and

transmit, to a computing device at the location, the current customer log comprising the facial template associated with the account of the particular user, wherein the computing device identifies the particular user based on identifying the facial template associated with the account of the particular user from the current customer log as being similar to a facial template of the particular user generated from a facial image of the particular user captured by the computing device.

Scope of the independent claims

8 In the pre-hearing report the examiner has raised concerns regarding the scope of the independent claims. Whilst not raising a plurality objection, the examiner has hinted that independent claim 1 and 12 may relate to one invention with independent

claims 7 and 17 relating to a second invention. However, as the examiner explains it is difficult to discern whether this is a plurality issue, an issue of clarity and conciseness, or both. In the absence of a plurality objection, Mr Williams in his skeleton arguments and at the hearing has directed his arguments towards independent claim 1 and as all the claims relate to the same invention their patentability follows.

9 Whilst the question of plurality is not before me, I consider the inventive concept (as discussed in greater detail below) of the specific interaction between the three different computing devices to enable the automatic hands-free identification of a user wherein one computing device broadcasts an identifier and then in order to obfuscate the identity of a user computing device, the user computing device does not directly communicate with the computing device but instead retransmits the identifier to another computing device to be present in each independent claim. It would appear to me that the issue, if any, is one of clarity and conciseness rather than plural invention.

The Issues to be decided

10 There are two issues to be decided in relation to the Application. Firstly, whether the invention as defined in the independent claims is inventive in light of two pieces of prior art. Secondly, whether the claimed invention relates to excluded subject matter, in particular whether the invention falls into one of the categories set out in section 1(2)(c) of the Patents Act 1977 as a method of doing business and/or a program for a computer as such.

The law

11 The examiner has raised objections under section 1(1)(b) and section 1(2) of the Patents Act 1977 that the invention does not involve an inventive step and is not patentable because it relates inter-alia to one or more categories of excluded matter. The relevant provisions of this section of the Act are shown in bold below:

12 Section 1(1) of the Act sets out what is required of a patentable invention as follows:

> *1(1) A patent may be granted only for an invention in respect of which the following conditions are satisfied, that is to say –*
>
> *(a) the invention is new;*
>
> ***(b) it involves an inventive step;***
>
> *(c) it is capable of industrial application;*
>
> ***(d) the grant of a patent for it is not excluded by subsections (2) and (3) or section 4A below;***

13 The provisions in relation to inventive step are found in section 3 which states:

> ***3. An invention shall be taken to involve an inventive step if 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).

14 The Court of Appeal in Windsurfing[1] formulated a four-step approach for assessing whether an invention is obvious to a person skilled in the art. This approach was restated and elaborated upon by the Court of Appeal in Pozzoli[2]. Here, Jacob LJ reformulated the Windsurfing approach as follows:

(1)(a) Identify the notional "person skilled in the art"

(1)(b) Identify the relevant common general knowledge of that person;

(2) Identify the inventive concept of the claim in question or if that cannot be readily done, construe it;

(3) 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;

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

15 The provisions in relation to excluded matter are found in section 1(2) which states:

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 –

(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.

16 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*[3], as further interpreted by the Court of Appeal in *Symbian*[4].

---

[1] Windsurfing International Inc. v Tabur Marine (Great Britain) Ltd, [1985] RPC 59
[2] Pozzoli SPA v BDMO SA [2007] EWCA Civ 588
[3] *Aerotel Ltd v Telco Holdings Ltd and Macrossan's Application* [2006] EWCA Civ 1371, [2007] RPC 7
[4] *Symbian Ltd's Application* [2008] EWCA Civ 1066, [2009] RPC 1

17 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.*

18 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*[5] and *Lantana*[6].

19 Lewison J (as he then was) in *AT&T/CVON*[7] set out five signposts that he considered to be helpful when considering whether a computer program makes a technical contribution. In *HTC* the signposts were reformulated slightly in light of the decision in *Gemstar*[8]. 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.*

20 It should be clear that the signposts are merely guidelines; although they provide a useful aid in assessing the technical character of a claimed invention, they were not intended to provide a definitive test (as Lewison LJ's obiter remarks in paragraph 149 of *HTC* make clear). Several judgments have emphasised this point - John

---

[5] *HTC Europe Co Ltd v Apple Inc* [2013] RPC 30
[6] *Lantana v Comptroller-General of Patents, Designs and Trade Marks* [2014] EWCA Civ 1463
[7] *AT&T Knowledge Venture/CVON Innovations v Comptroller General of Patents* [2009] EWHC 343 (Pat)
[8] *Gemstar-TV Guide International Inc v Virgin Media Ltd* [2010] RPC 10

Baldwin QC (sitting as a Deputy Judge) in *Really Virtual*[9] noted that the signposts, although useful, are no more than signposts and that there will be some cases in which they are more helpful than in others. Kitchin LJ made similar remarks in paragraph 51 of *HTC* that their usefulness does not mean they will be determinative in every case.

Arguments and analysis

21 At the hearing Mr Williams highlighted the salient points of claim 1 as being the first two clauses. The first two clause of claim 1 read as follows:

> *broadcasting, by a computing device, an identifier associated with the computing device at a location;*
> *receiving, by the computing device and from one or more other computing devices, one or more facial templates, each facial template associated with a corresponding user associated with a corresponding user computing device that received the broadcasted identifier at the location and retransmitted the identifier to the one or more other computing devices, each facial template comprising a representation of a respective facial image of the respective user*

22 He explained that the way the invention works is to use facial recognition to take images of users and to compare those images against templates to give a positive or negative indication as to whether that is the user.

23 Mr Williams explained that the invention works to orchestrate the interactions between three different devices – (i) a computing device (of the party, e.g. a merchant, wishing to do the identification); (ii) a user computing device (of the user being identified); and (iii) one or more other computing devices. It is this orchestration of the three devices that enables hands-free identification whilst providing security features and privacy benefits at the same time.

24 The merchant broadcasts an identifier from a location. The user computing device at the location receives the broadcast identifier and re-transmits the identifier to the other computing devices. If the user computing device re-transmits the identifier to the other computing devices, then the other computing devices transmit templates to the merchant computing device which allows the merchant to compare those templates with images they take at the location to enable them to identify the user. Mr Williams considers this to be the important part of claim 1 with the remainder of the claim relating to what the merchant does with the templates and capturing the images etc. The “new” part of the claim resides in the first two clauses which enables the subsequent parts to take place to obtain the advantages of the invention.

25 Mr Williams outlined the advantages of the invention. One advantage being the user computing device does not interact directly with the merchant computing device performing the identification. This provides additional privacy and security benefits to the user as it prevents the merchant computing device from gleaning or updating information from the user computing device that the user may not wish to share with the merchant/identifying party.

---

[9] *Really Virtual Co Ltd v UK Intellectual Property Office [2012] EWHC 1086 (Ch)*

26 Further as the other computing device is not the computing device performing the identification, the other computing device need not receive the contemporaneously obtained user images. Therefore, there is no computing device in the system of claim 1 that receives the images obtained of the user at the current time and the identification of the user computing device. This provides an additional advantage in privacy and security benefits to the user. Firstly, whilst the user has provided the other computing device with templates to enable user identification, that is not to say the user wants to provide the other computing device or the party operating the other computing device with a series of images obtained at different times and at different locations that could be used to build up a profile or time series of images of the user. Secondly, the user may wish to allow the merchant to perform an identification process but doesn't necessarily want the merchant to be able to identify every time the user enters a location e.g. their shop, with a particular computing device so doesn't necessarily want the merchant to have the user ID of the user computing device.

Inventive step

27 The examiner maintains that claims 1-5, 7, 10-15 and 17 are obvious in light of:

> D1: GB 2513173 A (JVE SOLUTIONS LTD.) in view of common general knowledge in the art; and
>
> D2: US 2013/0251216 A1 (SMOWTON et al.) in view of common general knowledge in the art

28 I will now consider whether invention as defined by the claims involves an inventive step using the Windsurfing/Pozzoli approach.

Step 1(a) and 1(b): Identify the notional "person skilled in the art" and their relevant common general knowledge

29 The first step is to identify the notional skilled person and their common general knowledge. The examiner has defined the skilled person as a designer or manufacturer of software used for identifying users at a location (for example at a merchant location).

30 The examiner considers the common general knowledge of the skilled person would include known identification means, including facial recognition (it being entirely conventional to require some form of identification in order to complete a transaction). The skilled person would also have knowledge of common proximity sensing means, such as via the use of Bluetooth® low energy beacons. Furthermore, the skilled person would be aware of the different conventional ways in which identification and transaction data can be captured, generated, stored, transmitted and received. The examiner argues that aspects of the common general knowledge are embodied in US2011/0178883 and US2015/0072618 which disclose a known way of detecting the mobile device of a user at a location is by the broadcast and retransmission of an identifier.

31 Mr Williams agrees with the examiner on these two points and I am also content to do so.

Step 2: Identify the inventive concept of the claim in question or if that cannot readily be done, construe it

32 The examiner has defined the inventive concept of the claims as relating to identifying users at locations by sending facial templates, associated with users, from computing devices (such as payment processing devices) to a local computer, so that facial recognition processing can be carried out at the local computer. The facial templates are only sent from the computing devices (where they may be stored either locally or remotely) to the local computer when a user device has received an identifier associated with the local computer and has retransmitted the identifier to the computing devices. A match between the received facial templates and facial templates which are captured by the local computer, is used to confirm the identity of a particular user (and therefore allows the completion of a transaction). The specific details relating to how the facial recognition is implemented are considered to be based on conventional facial recognition techniques and do not form the inventive concept.

33 Mr Williams argued that the inventive concept of the invention resides in a method which causes a user identification system to operate in a way that ensures that only facial templates associated with users 1) at the locations and 2) whose devices forward the received broadcast identifier to the other computing devices are received by the computing device and used to identify the user. The method allows for secure and efficient automated identification while still allowing the identification to be "hands-free". The inventive concept is therefore the particular operations which the particular hardware is caused to perform to carry out the task of automatic hands-free identification of a user.

34 It is clear the inventive concept does not lie in the hardware or the use of facial recognition in identifying a user. As highlighted by Mr Williams above the crux of the invention is defined in the opening two clauses of claim 1. In my opinion, the inventive concept lies in the specific interaction between the three different computing devices to enable the automatic hands-free identification of a user whilst also providing security features and privacy benefits discussed in paragraphs 23-24 above.

Step 3: 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

35 Mr Williams identified four differences between D1 and D2 and his definition of the inventive concept:

• the computing device broadcasting an identifier;

• the user computing device does not interact directly with the computing device, but retransmits the identifier to the other computing device;

• receiving one or more facial templates from the other computing device, where each template comprises a respective representation of a facial image of a respective user;

• the computing device receives only templates representing users of user devices that 1) are at the location, and 2) retransmitted the identifier to the one or more other computing devices.

36 From the arguments put forward in the pre-hearing report it appears the examiner agrees that neither D1 nor D2 disclose the differences outlined by Mr Williams. I am minded to agree.

37 As discussed by the examiner in the pre-hearing report, D1 discloses a system for authenticating an "acquirer" of a product or service from a product or service provider. The acquirer may download an application on a mobile device and register their details, including biometric identifiers, such as a photograph of the acquirer. The mobile device of the acquirer is detected at a location of a merchant **by any suitable means** (e.g. via a wireless communication network, including Bluetooth®) and associated with the acquirer, and subsequently the acquirer details. A merchant device uses a camera to capture images or a video of an acquirer at the location and compares the images received with the biometric data contained within the acquirer details (the processing can be done locally). If a match is found then the acquirer is authenticated and is able to pay for the products/services they ordered/complete a transaction (without needing to produce a payment card).

38 At the hearing Mr Williams explained the disclosure of D1 in the context of ordering a coffee from a coffee shop. The acquirer would set-up a number of preferred purchases within an app e.g. order a coffee whenever I get within 100m of a certain coffee shop, and then when the acquirer gets within 100m of the coffee shop the phone will send an order to the coffee shop automatically and dock payment by whatever means has been set. The acquirer then merely enters the coffee shop and collects their coffee. D1 further describes a method of identifying the acquirer when they arrive at the coffee shop to collect their coffee.

39 D2 is also concerned with allowing a merchant to identify of a user. As with D1, the communication between the merchant location and the user device is direct user to merchant communication. Either the user device is constantly scanning for the merchant or the merchant is constantly scanning for the user. D2 discloses a method of personal identification combining proximity sensing with biometrics. Proximity sensing, such as by using short-range radios (e.g. Bluetooth®) found in mobile devices, is used to identify customers that are physically nearby a location, such as a POS terminal. A video camera is used to capture biometric data of customers at a location and a list of IDs (related to the customers who were detected by the proximity sensing) and the biometric data is provided to an identification service. This data is used to produce a candidate set which corresponds to a ranked list of the most likely customers who are in proximity and based upon the facial recognition.

Step 4: Viewed without any knowledge of the alleged invention as claimed, do those differences constitute steps which would have been obvious to the person skilled in the art or do they require any degree of invention?

40 In the pre-hearing report the examiner has made it explicitly clear that the inventive step argument is not based on a mosaic of documents but rather that it would be obvious to the skilled person to modify either of D1 or D2 in light of the common general knowledge to arrive at the claimed invention.

41 Mr Williams considers the skilled person to have a clear understanding of what the identification system in D1 is all about. It is about making sure the user who tuns up at the merchant location is actually the user who placed the order. When the user arrives at the merchant location, the user is already well-known to the merchant and a transaction has already taken place between the two. The merchant already knows information about the user device that the user is carrying. Therefore, Mr Williams argues, there is no benefit and it would seem pointless to modify the system in D1 to introduce the system in claim 1 whereby the identity of the user computing device is actively obfuscated from the computing device and avoid direct communication between the two devices. Further D1 does not discuss privacy concerns at all and therefore the skilled person would have no motivation to modify it with privacy concerns in mind.

42 However, Mr Williams contends, even if the skilled person were minded to modify D1 to address some privacy concerns, it has not been shown that the common general knowledge (including the disclosures of both US2011/0178883 and US2015/0072618) of the skilled person includes a method by which one computing device broadcasts an identifier and then in order to obfuscate the identity of a user computing device, the user computing device does not directly communicate with the computing device but instead retransmits the identifier to another computing device. The other computing device subsequently supplying the templates to the computing device for identification of the user.

43 Mr Williams explained that D2 does discuss privacy concerns and addresses this through the use of an identification service. Once obtained by the merchant location, the user device ID and the images of the location are both provided to the identification service. It is the identification service that then matches up and says it could be this person or that person, here are your candidate sets. The way privacy is addressed so far as the merchant is concerned is that the merchant does not have the templates available at the merchant location and does not do the identification. As a result, the identification service does have access to the templates and does receive the time series of user images at different points in time which enables them to build up a broader profile of the user which is prevented in the claimed method. Therefore, D2 does provide a solution to privacy but it does not provide the additional security of none of the computing devices in the system receives the images obtained of the user at the current time and the identification of the user computing device.

44 Mr Williams further described how D2 also discusses privacy considerations which may make some customers unwilling to continually broadcast their device-unique identifier because it may be used to identify a user to anyone in range. D2 proposes two solutions to these concerns either by encrypting the device identifier or through the use of a two-step protocol whereby the user device first grants authorisation to the merchant location before supplying the device-unique identifier. Therefore, as D2 provides different solutions to the problem of privacy and security concerns, the skilled person is deprived of any motivation to look for further solutions in any other documents or the common general knowledge. In any event, the common general knowledge does not provide the broadcast, retransmission method of the claimed invention.

45 I am minded to agree with Mr Williams' arguments. I can see no motivation in D1 for the skilled person to seek to modify the authentication system to address any privacy concerns. Similarly, I can see no motivation in D2 for the skilled person to seek to modify the identification method to include different or additional privacy and security solutions to the ones offered in D2 itself. Furthermore, I agree that even if the skilled person were minded to seek to modify either D1 or D2 with privacy concerns in mind, I have nothing before me to suggest that the common general knowledge of the skilled person includes a solution of one computing device broadcasting an identifier and then in order to obfuscate the identity of a user computing device, the user computing device not directly communicating with the computing device but instead retransmitting the identifier to another computing device.

46 As discussed in paragraph 9 above, it appears to me that the inventive concept is present in each independent claim. Therefore I consider the independent claims to be inventive.

Excluded matter

Step 1: Properly construe the claims

47 The first step of the test is to construe the claims. In the pre-hearing report the examiner has taken the decision to focus on independent claims 1 and 12 in light of the drafting issues discussed in paragraph 8 above. At the hearing Mr Williams has also directed his argument towards independent claim 1. In the first instance I will therefore consider independent claims 1 and 12. I do not think this presents any real problem since both the applicant and the examiner appear to agree as to the meaning of these claims.

Step 2: Identifying the actual or alleged contribution

48 The examiner considers the contribution not to reside in the hardware to implement the invention. The hardware is entirely conventional. There is no disagreement from Mr Williams on this point. Therefore, the examiner argues any contribution lies in the programming of known hardware. The examiner states that what has actually been added to human knowledge lies in the specific way in which particular data is transmitted, received and stored by the various computing devices.

49 However, Mr Williams disagrees with the examiners assessment of the contribution and does not consider it to lie in aspects of the programming. Mr Williams considers the contribution to be a new way of providing hands-free identification that is secure and efficient. This is provided in the method of claim 1 by the computing device broadcasting an identifier, the user computing device not directly communicating with the computing device but instead retransmitting the identifier to another computing device, and the other computing device providing templates to the computing device to enable identification of a user to take place.

50 I am persuaded by Mr Williams' assessment of the contribution and I am happy to adopt it.

Steps 3 and 4: Does the contribution fall solely within excluded matter/is it technical in nature?

51 What I must now decide is whether the contribution identified above relates solely to a program for a computer as such and/or a method of doing business as such. This corresponds to step three of the Aerotel test.

52 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".

Mental Act

53 Whilst the examiner has not formally raised any argument to the contribution falling within the mental act exclusion, the examiner in the pre-hearing report has stated that when considering improved user identification or recognition in a general sense, it is important to note that methods for facial recognition, or determining identification by other means, are in themselves not regarded as technical. When computer implemented they relate to computer programs as such, or otherwise to mental acts.

54 Mr Williams therefore addressed the mental act exclusion at the hearing. I agree with Mr Williams' argument that the mental act exclusion is be interpreted narrowly as made clear by HHJ Birss in *Halliburton*[10]. It only covers acts that are carried out by "purely mental means" and does not extend to those which are merely capable of being performed mentally. the exclusion was to prevent patents being granted which could be infringed "by thought alone". HHJ Birss specifically outlined that, with this interpretation, a claim carried out on a computer could not be excluded as a mental act. Therefore, if a computer, or any other hardware, is involved in the invention, which is clearly the case here, it will not be excluded as a mental act.

Computer program

55 Mr Williams contends that the method of claim 1 relates to the real-world application of user identification and finds direct application in any situation in which it is desired to automatically identify users without the user needing to produce identification documents. He submits that the configuration and operation of computing devices to perform authentication of individuals is plainly a technical task that falls outside of the exclusions set out in section 1(2). Step 3 of the test requires us to ask whether the contribution falls solely within excluded subject matter. Referring again to *Halliburton*, HHJ Birss states at paragraph 71:

> *"Is it more than a computer program as such? The answer is plainly yes. It is a method of designing a drill bit. Such methods are not excluded from patentability by Art.52 and s.1(2) and the contribution does not fall solely within excluded territory. Drill bit design is not a method of doing business, nor a scheme for playing a game nor (as I have held) is this claim a scheme for performing a mental act."*

[10] Halliburton Energy Services Inc's Applications [2012] RPC 129

56 Following this reasoning Mr Williams submits that the method of claim 1 is plainly more than a computer program as such. It is a method of identifying users.

57 I will now consider the *AT&T/CVON* signposts as an aid to determining whether the contribution makes a technical contribution. Mr Williams explained the signposts are only signposts and sitting above them has to be the overriding consideration of the law and what is a computer program as such and he submits that the contribution is clearly not a computer program as such. I agree but in this case I feel consideration of the signposts will have some benefit in determining whether a technical contribution has been made.

58 Mr Williams highlighted signposts (i), (iii), (iv) and (v) as being met by the contribution. I agree that the second signpost is clearly not met.

59 With regard to signpost (i), Mr Williams argues the task of automatically identifying a user is not a task that is carried out solely within the computer, but requires the retrieval of, and processing of, images from the "real-world", to provide an identification of a user in the "real world". I am minded to agree. In my view, the issue of security and privacy for users when using computing devices is a technical problem which has an effect outside of the computer/computer system. The method of the of identifying users makes a technical contribution by providing additional security and privacy benefits to users.

60 Turning to signposts (iii) and (iv) I do not agree with Mr Williams' argument that the user identification system is clearly caused to operate in a new way as compared with the prior art user identification systems which results in an increase in the speed and reliability of the computer. I agree with the examiner's view that even though the claimed invention is novel, it does not mean the computer is operating in a new way. If it did then it is hard to see the exclusion as having any real meaning. Rather what signpost (iii) is referring to is a new way of operating the computer in a technical sense. It is not about new ways of handling particular types of information nor is it about the functional interrelationships between various components that are necessary to implement a new method of identifying a user in order to authenticate financial transactions. Further with regard to signpost (iv), the computer itself is not operating more efficiently or effectively. Rather it is operating in much the same way as before albeit it is being asked to do something different.

61 I disagree with Mr Williams that signpost (v) is met. The contribution provides an improved method of automatically identifying users whilst providing the security and privacy benefits discussed above. In my view, the broadcast, retransmission scheme of the claimed invention is merely circumventing the security issues associated with direct contact between the user computing device and the merchant computing device by removing the contact rather than solving the stated problems.

62 Looking at the fourth step, as discussed above I consider the contribution to be technical in nature.

Business method

63 Looking at the application as a whole to analyse what the method does externally to the computer system, the method provides a way of identifying and authenticating

customers using facial recognition, or other identification means, in order to perform business transactions (such as financial transactions) whilst providing the user with additional security and privacy benefits. Whilst authorising a transaction is a fundamental economic practice, used for conducting business and the hardware required for carrying out the invention is entirely conventional, the way in which the hardware is utilised provides a new or more secure method of identification or authentication, such that there is, in my view, a technical contribution. I do not consider a contribution made in providing users with privacy and security benefits to lie solely within the business method exclusion.

Other Office decisions

64 During the hearing Mr Williams made reference to the previous Office decision O/390/17 which he considers to have similarities with the present application. In the decision a radar system capable of localizing airborne targets was considered to not be excluded. I am not bound to follow the Hearing Officer's decision in this case and having considered it I am satisfied that there are sufficient differences between the present application and the decision that nothing is to be gained from further consideration thereof. As Pumfrey J said at paragraph 186 in *Research in Motion*[11]:

> *"little or no benefit is to be gained by drawing analogies with other cases decided on different facts"*

Outstanding issues

65 Other than inventive step and excluded matter, I note there are other issues outstanding on this application such as full substantive examination and updating of the search.

Conclusion

66 I find that the claimed invention involves an inventive step under sections 1(1)(b) and I do not consider the contribution made by the claimed invention to be excluded as a computer program or business method under section 1(2). I therefore remit the application to the examiner for further processing.

Appeal

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

C. L. Davies
Deputy Director, acting for the Comptroller

[11] *Research in Motion UK Ltd v Inpro Licensing* [2006] RPC 20