Intellectual Property Office

BL O/886/22

12 October 2022

PATENTS ACT 1977

APPLICANT	Cyacomb Limited
ISSUE	Whether patent application GB 1705333.1 complies with section 1(2) of the Act
HEARING OFFICER	Dr L Cullen

DECISION

1 This decision concerns patent application GB 1705333.1 entitled *"System and method for management of confidential data"* in the name of Cyacomb Limited.

2 The matter to be decided is whether the invention as claimed in this application relates to matter excluded from patentability as defined in section 1(2) of the Patents Act 1977 (hereafter "the Act").

Introduction

3 This patent application was filed on 3 April 2017, with no claim to priority and with a request for search. The search examiner declined to perform a search and issued an Examination Opinion dated 14 September 2017 explaining that the invention was a computer program as such and therefore was excluded from patentability under the Act. The application was published on 10 October 2018 as GB2561176A, and substantive examination was subsequently requested within the prescribed time period.

4 During substantive examination of this application, an equivalent international application was identified, published under the Patent Cooperation Treaty as WO 2018/185456. An International Search Report and an International Preliminary Report on Patentability (IPRP) are available for WO 2018/185456. The IPRP identified three prior art patent documents in support of objections that all the claims lacked novelty and/or an inventive step. The UK examiner made use of these documents to raise similar objections and reiterated the objection made previously in the Examination Opinion that the invention was excluded from patentability as a computer program as such.

5 The application was successfully amended to overcome the novelty and inventive step objections. However, arguments presented as to why the invention goes beyond a computer program as such were not successful in overcoming the exclude matter

objection raised by the examiner. A further round of correspondence between the applicant and the examiner provided no resolution such that in the final examination report of 21 March 2022 the examiner offered a hearing. The applicant accepted and a pre-hearing report was issued by the examiner on 31 March 2022, setting out the matter to be resolved and a summary of the arguments that had been raised in relation to this matter.

6 In a request from the Office dated 22 June 2022, on my behalf as the Hearing Officer, the applicant was asked to address two matters at the hearing: i) the contribution to the art made by the invention; and ii) how the invention works in a subset of embodiments where a secure element is based on a fragment of a data element. Skeleton arguments were provided by the applicant on 8 July 2022 and included content addressing both matters. It was helpful to have these arguments in advance of the hearing and I would like to extend my thanks to the applicant for providing them.

7 The hearing took place on 18 July 2022 by video conference. It was attended for the applicant by their attorney, Dr Craig Hutchison of Lawrie IP, and by his colleague Mr Simon Black. Dr Andrew Hughes was present as assistant to the hearing officer, and the examiner also attended.

8 As such hearings are open to the public, a number of observers were also present for training purposes.

The Invention

9 The invention arises in the context of enabling a confidential database to be interrogated without exposing the records themselves to the interrogating party, thereby maintaining the confidentiality of the database. Applications are envisaged in fields such as law enforcement and the searching of commercially sensitive data.

10 The invention uses a “representation database” which notionally sits between the confidential database, held by a first entity, and a second entity who wishes to interact with the database in some way. The representation database comprises one or more “secure elements”, each of which are obfuscated representations of a dataset present in the confidential database. By way of example, a specific dataset might be passport numbers, of which there may be many contained within the records of the confidential database. The passport numbers are grouped together and processed by an obfuscating operation with the result that they cannot be read by the second entity or, for that matter, by any third party if they were to obtain the secure element. The secure element can, however, be searched by a party who holds a specific passport number and knows what obfuscating operation was applied, thereby to establish whether that specific passport number is represented in the secure element. A negative result, that is to say no match between the queried passport number and the secure element, indicates that the passport number is not present in the confidential database. Depending on how the invention is implemented, a positive result, that is to say a match between the queried passport number and the secure element, will indicate that the passport number is, or may be, present in the confidential database. Suggested implementations are via a Bloom filter or a Cuckoo filter, which give rise to a small

proportion of false positives and therefore introduce an element of uncertainty as to the veracity of any positive result.

11 Preferably, but not essentially, the records are obfuscated by an operation that is irreversible, thereby to make it impossible to derive the original data from the representation database. Suitable methods of obfuscation include encryption and hashing. "Hashing" is a preferred technique, in which a unique data string (the "hash") is derived from the dataset via a hashing algorithm. The representation database, in this case, would comprise a hash for each secure element.

12 The application as filed describes various operations which can be applied to the representation database. With regards to management of the secure elements, it describes the addition of a secure element to the representation database, the merging of secure elements present in the representation database, and the updating of a secure element present in the representation database. With regards to interrogation of the representation database, the idea is that a requesting party in possession of a piece of data, which I shall call the "query data", can derive the hash (for example) of that data and search the representation database for a match. If such a match is forthcoming, the requester can infer that their query data is present in the confidential database (possibly subject to the uncertainty mentioned above caused by false positives). Critically, at no point are they provided access to the confidential database itself.

The Claims

13 The application as currently on file, following amendment, has a total of thirty-eight claims. There are three independent claims to methods of data management, claim 1, claim 28 and Claim 29.

14 Claim 1 concerns the scenario of interrogating the representation database. It is characterised by a portion of the representation database being sent to the requesting party, such that they can interrogate it using their own computers as opposed to those of the holder of the full representation database. Claims 28 and 29 concern management of the secure elements of the representation database; claim 28 is directed to adding a secure element to the representation database and claim 29 is directed to updating a secure element in the representation database. The arguments presented during the hearing focussed particularly on claim 1 as amended. My discussion below also includes claim 28 and claim 29.

15 Claim 1, as amended, reads as follows:

> *1. A method of data management for a system for identification of digital content elements, the method comprising:*
>
> *creating a representation database which comprises at least one secure element, the at least one secure element being a secure representation which corresponds to a certain characteristic of at least a fragment of a confidential data element of at least one dataset stored in at least one database, wherein the at least one dataset contains the confidential digital content;*

receiving at least one data request from a requesting entity, the data request being associated with at least one secure element;

processing the at least one data request by identifying at least a portion of a representation database associated with at least one secure element;

and providing at least one processing result by transmitting the identified portion of the representation database to the requesting entity, thereby to enable processing at the requesting entity wherein the requesting entity is able to utilise the secure elements to detect the presence of specific data elements without having access to the original data elements.

16 Claim 28, as amended, reads as follows.

28. A method of data management for a system for identification of digital content elements, the method comprising:

receiving a management request, the step of receiving comprising receiving a first secure element, the first secure element being a secure representation of at least one dataset stored in a first database;

processing the at least one management request by performing at least one operation on a representation database;

wherein the representation database comprises at least one secure element, the at least one secure element being a secure representation of at least a fragment of a confidential data element of at least one dataset stored in at least one database, wherein the at least one dataset contains confidential information and

wherein the step of processing comprises:

adding the first secure element with the representation database wherein

the step of adding comprises performing a bitwise logical OR operation on the first secure element and at least one secure element comprised in the representation database; and

providing at least one processing result.

Presumably the receiving step of the method should recite *"receiving <u>at least one</u> management request"*, to render it consistent with the processing step, which refers to *"at least one management request",* and also with claim 29.

17 Claim 29, as amended, reads as follows:

29. A method of data management for a system for identification of digital content elements, the method comprising:

receiving at least one management request comprising at least one updated version of a secure element;

processing the at least one management request by performing at least one operation on a representation database;

wherein the representation database comprises at least one secure element, the at least one secure element being a secure representation of at least a fragment of a confidential data element of at least one dataset stored in at least one database, wherein the at least one dataset contains confidential digital content;

wherein the step of process in, [sic] *comprises updating the representation database to include the updated version of the secure element and providing at least one processing result."*

The final part of the claim is plainly intended to concern *"the step of processing."*

The Issue to be decided

18 The issue to be decided is whether the invention as claimed relates to matter excluded under Section 1(2) of the Act, specifically part (c).

19 I note that the examiner has not performed a search under section 17 of the Act so, should I find in favour of the applicant in relation to excluded matter under section 1(2), the application would need to be remitted to the examiner for further consideration.

The Law

Excluded Matter – Section 1(2)

20 Section 1(2) of the Act sets out certain categories of subject-matter which are not considered to be inventions. These categories are often referred to as 'excluded subject-matter'.

21 The relevant provisions of section 1(2) of the Act are shown with added emphasis 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 –*
>
> *(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****.*

22 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 that court 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. These steps are:

(i) properly construe the claim;

(ii) identify the actual contribution;

(iii) ask whether it falls solely within the excluded subject-matter;

(iv) check whether the actual or alleged contribution is actually technical in nature.

In *Symbian,* the Court of Appeal made it clear that the four-step test in *Aerotel* was not intended to be a new departure in domestic law; it confirmed that the test is consistent with the previous requirement set out in case law that the invention must provide a *"technical contribution"*.

23 Kitchen LJ noted in *HTC*[3] that the *Aerotel* test is followed in order to address whether the invention makes a technical contribution to the art, with the rider that novel or inventive purely excluded matter does not count as a "*technical contribution*". Thus, the question of whether a computer-implemented invention is patentable has to be resolved by asking whether it reveals a technical contribution to the state of the art and this question is answered with the aid of the four-step test for excluded subject-matter set out in *Aerotel*.

24 According to paragraph 46 of *Aerotel*, applying the 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 thus will not, as the fourth step puts it, be "*technical in nature*".

25 Lewison LJ provided five signposts in *AT&T/CVON*[4], which he reformulated in *HTC*[3] in light of the decision in Gemstar[5], which he considered helpful when exploring the

---

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

[2] *Symbian Ltd v Comptroller-General of Patents [2009] RPC 1*

[3] *HTC Europe Co Ltd v Apple Inc [2013] EWCA Civ 451; the "rider" is at paragraph 35*

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

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

issue of whether (or not) a computer programme makes such a technical contribution. These so-called "*AT&T 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; and

v) whether the perceived problem is overcome by the claimed invention as opposed to merely being circumvented.

26 I note that there is no disagreement between the applicant and the examiner over the relevant law.

Overview of the applicant's arguments

27 The applicant's arguments were presented by Mr Black, with much of the ground he covered having been foreshadowed in the skeleton arguments submitted in advance of the hearing.

28 To provide context for the invention Mr Black described the applicant's view of how, in the prior art, confidential data is typically shared with a requesting party: the data is encrypted and sent to the requesting party; then the requesting party decrypts the data and searches it. This approach was said to have two significant disadvantages:

i) the encrypted data may be intercepted during transmission, potentially leading to the unwanted spread of the data and putting it at risk of being decrypted by an unauthorised party, and

ii) the requesting party has full access to the data following its decryption, thereby exposing the data to a risk of theft or misuse.

These disadvantages were said not to arise with the present invention.

29 With regards to (i) the risk during transmission, in the present invention, it is only a portion of the representation database that is transmitted (to recap, the representation database is the obfuscated database derived from the confidential database). The worst-case scenario here in the case of intercept is that an obfuscated portion of the confidential data is exposed. For the preferred embodiment, in which the obfuscation has been achieved by an irreversible operation, the potential impact is further mitigated because it would not be possible to derive anything of value from the data without knowledge of the obfuscating operation that had been applied.

30 With regards to (ii) the use by the requesting party, the present invention permits the requesting party to interrogate the received portion of the representation database to establish the presence or absence in the confidential database of one or more pieces of query data, whilst preventing them from reading the data.

31 These two aspects were said to provide a more secure method of interrogating a database, enabling data to be shared without providing access to the (confidential) data themselves or to the confidential database in which the data are held, thereby maintaining the security of the database. Mr Black said that the invention improved the security of an interaction between two computers. He characterised the representation database as "*a separate resource*", sitting between the confidential database and the requesting party. Moreover, the method had universal applicability in that it could be used with data of any type or form. He argued that these were indications of a technical nature such that, whilst it is computer-implemented, the invention amounted to more than a program for a computer as such.

32 The arguments offered by the agent in relation to the five AT&T signposts and how they apply in this case are summarised in the relevant discussion below.

Analysis

33 To decide whether the invention concerns subject matter that is excluded from patentability, I must apply the four-step test that was set out by the Court of Appeal in *Aerotel.*

Step (1): Properly construe the claim

34 The first step of the *Aerotel* test is to construe the claim, which is to interpret the claim through the eyes of the skilled person in light of the specification as a whole.

35 As mentioned above, the claims as amended and currently on file include three independent method claims. The examiner and the applicant consider that the claims as amended "are clear". I agree with this up to a point but I believe that it is necessary to note that there are some differences between claims 1, 28 and 29 that will have an impact on how they are construed. Unlike claim 1, claims 28 and 29 do not require the step of creating the representation database. While the discussion at the hearing focused predominantly on the invention as claimed in claim 1, I will begin the process of construing these claims by looking at the common features between them and the then turning to the additional features that make up claim 1. I will then consider claims 28 and 29.

36 The methods of claims 1, 28 and 29 share the following common features, numbered for ease of reference:

> *A method of data management for a system for identification of digital content elements, the method comprising:*
> *a) receiving at least one request [associated with* (claim 1) */ comprising* (claims 28 and 29)*] a secure element;*

b) *processing the request by performing at least one operation on a representation database;*
c) *wherein the representation database comprises at least one secure element, the at least one secure element being a secure representation of at least a fragment of a confidential data element of at least one dataset stored in at least one database, wherein the at least one dataset contains confidential digital content*
d) *and wherein the step of processing comprises providing at least one processing result.*

37 All three claims are directed to *"A method of data management…."* The description and drawings describe a variety of actions that can be applied to the representation database; for example, secure elements can be added (figure 5), merged (figure 9) or updated (figure 21); a portion of the database can be identified and extracted (figures 11 and 17); or the database can be searched directly (figure 13). Claim 1 concerns identifying and extracting a portion of the representation database; claim 28, concerns adding a record to the representation database; and claim 29, concerns updating a record in the representation database.

38 Feature (a) above concerns a request; in claims 28 and 29, it is *"a management request"* whereas in claim 1 it is *"a data request."* The data request of claim 1 is a request for data (even if it ends up being a lot of data); the management requests of claims 28 and 29 are for operations on the data – an insertion or an update – the results of which are then returned. For the purposes of establishing the inventive concept and the technical contribution, I do not consider that anything turns on this difference. I will refer below to both types as a 'request'.

39 Feature (a) further requires that the request be associated with, or comprise, a secure element. The term "*secure element*, is used consistently throughout the specification to mean a secure representation of a fragment of a confidential data element, or of a complete confidential data element, or of a whole dataset of confidential data elements of a single type. The secure element in this instance is one of a possible plurality of such elements associated with the request, To readily identify the specific secure element(s) of the request, as opposed to the secure element(s) of the representation database, I shall refer to it as '*the secure element(s) of interest to the requesting entity'.*

40 Feature (b) (i.e., *"processing the request by performing at least one operation on a representation database"*) is self-explanatory.

41 Feature (c) defines the representation database as comprising at least one secure element. The secure element is then defined in each claim as *"a secure representation which corresponds to a certain characteristic of at least a fragment of a confidential data element of at least one dataset stored in at least one database."* By contrast, paragraph 8 of the description gives a narrower definition, referring to the *"secure element being a secure representation of at least one dataset stored in at least one database."* The additional options provided for in feature (c) are based on the disclosure of paragraph 27 of the description, which refers to fragments of data elements. As noted in relation to feature (a) already, the inclusion of these fragment-based options means that the secure element within the representation database may be a representation of a fragment of a confidential data element, or of a complete

confidential data element, or of a whole dataset of confidential data elements of a single type.

42 Feature (d), (i.e., "*the step of processing comprises providing at least one processing result*") is self-explanatory.

Construing Claim 1

43 Claim 1 adds to the common features (a) – (d) identified above by introducing the step of creating the representation database. Furthermore, in relation to feature (b) the processing step involves identifying a portion of the representation database associated with the secure element of interest to the requesting entity and in relation to feature (d), the providing step involves transmitting the identified portion to the requesting entity.

44 Thus, I arrive at the following construction of this claim:

> *A method of data management for a system for identification of digital content elements, the method comprising:*
>
> *(1) creating a representation database which comprises a secure element derived from a dataset in a confidential database;*
>
> > *the secure element being a secure representation which corresponds to a certain characteristic of at least a fragment of a confidential data element of at least one dataset stored in at least one database, wherein the at least one dataset contains the confidential digital content*[6]
>
> *(2) receiving a data request from a requesting entity, the data request being associated with a secure element of interest to the requesting entity;*
>
> *(3) processing the data request by identifying a portion of the representation database associated with the secure element of interest to the requesting entity; and*
>
> *(4) providing a processing result by transmitting the identified portion of the representation database to the requesting entity,*
>
> *thereby to enable processing at the requesting entity wherein the requesting entity is able to utilise the secure element of interest to detect the presence of specific data elements without having access to the original data elements.*

45 So, the claim is to a method which provides for the creation of a representation database and then transmitting an identified portion of it to a requesting entity. As mentioned previously, for the requester to search for a match in the secure element they need to know by what obfuscating operation the secure element was derived from

---

[6] *There is no antecedence in the claim for "the confidential digital content", but it's meaning is apparent.*

the original dataset. I therefore asked Mr Black how the requester is able to know this. He explained that it is communicated to them as a precursory step that is not considered to be critical for the purpose of defining the invention. I am content to accept this point and therefore to retain the approach of claim 1 of omitting the precursory communication from the method.

46 It was not immediately clear to me whether the first two steps of claim 1 – creating the representation database and receiving a data request – must occur in that order. However, in light of the above-mentioned precursory communication the requesting entity will be aware of what secure element to frame their request with. In their letter dated 17 December 2021, the attorney acting for the applicant, made clear that the creation of the representation database is the first step and that the request for the requesting entity occurs after creation of the representation database. I am content to proceed on this basis.

47 The final portion of the claim (i.e. "*thereby to enable processing at the requesting entity wherein the requesting entity is able to utilise the secure element of interest to detect the presence of specific data elements without having access to the original data elements)* refers to a desirable result to be achieved in the sense that the resulting transmitted portion of data referred to in step 4 must be suitable for analysis by the third-party requester. This portion of the claim provides context for the preceding steps, but it does not specify any further steps in the claimed method. I therefore consider that it does not provide a material restriction to the scope of the claim.

Step (2): Identifying the actual contribution

48 The critical considerations when identifying the contribution were identified by Jacob LJ at paragraph 43 of *Aerotel*.

> *"The second step – identify the contribution – is said to be more problematical. How do you assess the contribution? Mr Birrs submits the test is workable – it is an exercise in judgment probably involving the problem said to be solved, how the invention works, and 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 – which is surely what the legislator intended."*

49 The contribution, therefore, is identified against the backdrop of the prior art, some knowledge of which is provided by the results of the search conducted on the equivalent international application. Each of the five identified documents describe the use of a hash of query data to search for a match in one or more hashes derived from confidential data. It follows that the broad concept of using obfuscated elements, such as hashes, to securely search confidential databases, is not new and therefore does not itself form the contribution. The contribution must therefore lie in the detail of the claimed method.

50 Any method steps which are precursory, or otherwise non-essential, would not be an essential part of the invention and thus should not form part of the contribution.

51 A simple way to assess this is to work backwards through the claim, looking to see if each step has a direct functional link with the preceding step. Step four involves

transmitting an identified portion of the representation database, which is therefore directly linked to step three in which the portion is identified as that which is associated with the secure element of interest. The secure element of interest is known from the data request, which is received in step two, thereby providing a link between steps three and two. The secure element associated with the data request makes sense only if there is at least one secure element present in the representation database, but is that sufficient to provide a direct functional link?

52 Representation databases as such are not new. The first document identified in the international search report, US 2014/281578 (Bennison), teaches a database of "*cryptographically hashed values*" which sits between a confidential database and a requesting party, fulfilling the role of a representation database even though not named as such.

53 As noted above, the full definition of the secure element permits the secure element to be a representation of a fragment of a confidential data element, or of a complete confidential data element, or of a whole dataset of confidential data elements. The Bennison prior art discloses the complete data element type but has not been shown to disclose either the fragment type or the dataset type of secure element.

54 Were the use of all three types of secure element in representation databases to be standard then one could argue that the step of creating the representation database was merely a precursor to the invention and could therefore be excluded from the contribution; however, with that not having been established, I think it reasonable to include the step of creating a representation database of at least one secure element as a necessary part of the invention.

55 The problem addressed by the presently claimed invention is how to interrogate a remote representation database whilst ensuring the queries themselves remain confidential. The invention works by creating an appropriately constructed representation database, a portion of which is identified from a data request and transmitted to the requesting entity, such that the database portion can be interrogated using the requesting entity's own computer. It has the advantage that the queries are confined to that computer and so are not available to the holder of the database and are not at risk of being intercepted during transmission. The examiner's definition of the contribution, as set out at paragraph 25 of the pre-hearing report, captures these aspects. Furthermore, at the hearing Mr Black accepted that identifying and transmitting of a portion of the representation database are essential components of the contribution.

56 It is common ground that the invention is implemented entirely by computers, so I accept the examiner's characterisation of the contribution as a computer-implemented method.

57 In light of the above considerations, I consider the contribution of the invention as claimed in claim 1 to be:

> *A computer-implemented method of processing a request from a requesting entity to a representation database which contains secure elements that are secure representations of confidential data elements stored within a confidential database, wherein*

the output of the processing of the request is an identified portion of the representation database which is sent to the requesting entity such that the secure elements can be used to detect the presence of specific data elements without having access to the original data elements.

the secure database is created prior to the receipt of the request

the secure element is a representation of a fragment of a confidential data element, or of a complete confidential data element, or of a whole dataset of confidential data elements.

Step (3): Is there any contribution outside the excluded categories?

58 A computer-implemented invention necessarily involves a computer program; however, whether the invention amounts to a computer program as such, and is therefore excluded from patentability, is determined by whether the contribution to the art has a technical nature. This can be assessed by testing the contribution against the five AT&T signposts which are indicative of a technical effect in computer-implemented inventions[3,4].

59 The *first AT&T signpost* asks whether there is a technical effect on a process which is carried on outside of the computer. As proposed, the contribution indicates that there is a communication between the computer of the requesting entity and that of the host of the representation database. Mr Black argued that the invention provides a more secure interaction between the host computer and the requester's computer, one that is less vulnerable to hacking, and that this amounted a technical effect outside of the computer. It would appear that the applicant has relied upon the transfer of data taking place outside of the computer system holding the original secure database.

60 In support of the opposing view, the examination reports referred to the precedent provided by paragraph 30 of *Lantana*[7], wherein an arrangement of two computers connected by a telecommunications network was considered to be "*an entirely conventional computing arrangement"* falling within the scope of *"the computer"* in relation to the first signpost.

61 It is pertinent here to distinguish between the characteristics of the computer arrangement itself and the characteristics resulting from the software running thereon. The physical connection between the computers is a conventional one which is not made more secure by the invention, and indeed Mr Black did not suggest as much. He pointed to the interaction between them, which in this case is the request for data and the return of data. This interaction is something that is determined by the software running on the computers and does not reflect any modification of the computers themselves. Since those computers are conventional computers, I consider them to fall within "*the computer*" of the first signpost. Thus, even if I were to accept the proposition that the contribution requires the presence of two computers connected together, it would still follow that there is no process going on outside of the "*the computer*" of the signpost, so there cannot be a technical effect on such a process.

[7] *Lantana Ltd. v Comptroller General of Patents*, [2013] EWHC 2673 (Pat)

Whilst the invention may provide for a more secure interaction, it does not meet the first signpost.

62 The *second AT&T signpost* asks whether there is a technical effect operating at the level of the architecture of the computer. This signpost requires consideration as to what the computer program actually does to the computer system itself. What is the effect at the level of the architecture? With reference to the *AT&T/CVON* judgment at paragraphs 21-34 (which referred to the EPO Technical Board of Appeal decision in IBM (T 0006/83)[8] and concerned an improved method of communication between programs and files held at different processors within a known network), an invention is patentable under s.1(2)(c) if it works irrespective of the nature of the data and it is considered to relate to the architecture of the system, i.e. how the componentry (i.e., the physical components of the system) are interconnected.

63 Mr Black argued that the presence of the representation database interposed between the requester's computer and the confidential database, amounted to a new architecture. The change in relationship between the third-party requester and the data owner is depicted in the prior art arrangements of figure 1 versus the embodiments of the present invention as shown in, for example, figure 3. It is argued that the present invention has an inherently different architecture because data requests are processed via a representation database rather than the original secure database. While this certainly characterises the "architecture" of the data management system used in the invention, the architecture of a computer refers to its componentry as opposed to the software run by that componentry. The invention provides a particular way to interrogate a database, a way that would be implemented by a software application running on the computer; it has no effect at all on how the components of a computer operate and thus does not operate at the level of the architecture of the computer. It follows that the second signpost is not met.

64 The *third AT&T signpost* asks whether the computer is being made to operate in a new way. It was proposed that the invention works in a new way and is carried out by a computer, thus the computer works in a new way. Lewison LJ has previously explained that this signpost is directing towards *"some generally applicable method of operating a computer rather than a way of handling particular types of information"*[4], which is pertinent here. The present invention is directed to the secure handling of confidential information, whilst a computer performing the invention operates in a conventional manner to run the software by which the invention is delivered. Accordingly, the computer is not made to operate in a new way and so the third signpost is not met.

65 The fourth *AT&T signpost* relates to whether the program makes the computer run more efficiently and effectively. Again, the courts have held that it is the computer *as a whole* which must be better, not just the application running on the computer. The effects of the present invention are confined to how confidential information is shared; they have no impact on how the computer performs other tasks. In their submissions, the attorneys highlighted how the invention reduces the necessary storage and the number of installations on the computer. The applicant argued that allowing a requesting entity to perform processing on an identified portion of the representation

[8] *IBM (T 0006/83) (Data processor network)*

database without necessitating the transfer of information relating to the specific service elements improves the security of the computer system. It was further argued that such improvements in data security make a computer system run more efficiently and effectively. However, in *Autonomy Corp Ltd*[9], it was found that *"The mere fact that a computer program reduces the load on the processor or makes economical use of the computer's memory or makes more efficient use of the computer's resources does not amount to making a better computer, and thus does not take it outside the category of computer program as such".* Accordingly, I consider that the fourth signpost is not helpful.

66 The *fifth AT&T signpost* requires that the identified technical problem is overcome rather than merely being circumvented. In considering the contribution above, I identified that the problem addressed is how to interrogate a remote representation database whilst ensuring the queries themselves remain confidential. The applicants in their submissions about the technical contribution have asserted that the problem to be solved was: *"Allowing access to confidential data without allowing third party access to the original secure database upon which it is stored."* However, as the applicants have acknowledged, this contribution is achieved by *"creating a representation database…which is a secure representation…of at least one dataset stored in at least one database…"*. It is thus clear to me that at no time is the third party allowed access to the original confidential, secure database. Instead, the third party is allowed access to a separate derivatised representation database. The problem of allowing access to 'confidential data' is thus circumvented by offering a representation of that data instead. For this reason, consider that the fifth signpost does not help.

67 The AT&T signposts therefore indicate that the computer-implemented contribution of claim 1 does not involve a technical effect.

Step (4): Check whether the contribution has a technical nature

68 Although *Aerotel* indicated that this step is liable to have been covered during the preceding step, and therefore may not be necessary, it is a useful prompt to take a step back from the structured approach and assess what is innovative about the claimed invention and ask whether, when viewed through that lens, there might be something technical in the nature of the invention.

69 It seems to me that the claimed method has three distinct aspects. First is the use of a representation database, which serves to maintain the confidentiality of the data. Second, is the population of the representation database with one or more secure elements, each derived from a confidential dataset, which may render the identification and searching of a portion of the representation database more secure than would otherwise be the case. Third is the moving of a portion of the representation database to the requester's computer, which enhances the privacy of the search queries applied because they do not need to leave the requester's computer. Each aspect therefore serves a different purpose and provides a different benefit; combined, they provide an arrangement to securely interrogate a confidential database. It may indeed be a better arrangement than that which has existed before, but there is no indication that these

[9] *Autonomy Corp Ltd v Comptroller General of Patents, [2008] EWHC 146 (Pat)*

aspects interact to solve a technical problem. I therefore find that this invention lacks a technical nature.

70 I find support for this conclusion in the decision of the Comptroller in *Datanovation Ltd.'s Application* (BL O/044/15)[10] where the hearing officer found that a computerised method for generating a database application that can be used to access an existing database allowing for example a search to be carried out in the database, the results to be displayed and data held in the database to be manipulated was found to be excluded as a computer program as such.

The later independent method claims – claims 28 and 29

71 Claims 28 and 29 are directed to methods of managing the content of a pre-existing representation databases. .

Step 1: Construing Claim 28 & 29

72 In light of the discussion above in relation to the common features of the independent claims and the additional features that characterise each claim, for Claim 28, in relation to feature (b) the processing step involves adding a secure element to the pre-existing representation database using a bitwise logical OR operation and in relation to feature (d), the providing step involves transmitting the identified portion to the requesting entity. This claim does not include the step of creation of the representation database.

73 For Claim 29, in relation to feature (b) the processing step involves updating the representation database to include an updated version of the secure element and in relation to feature (d), the providing step involves transmitting the identified portion to the requesting entity. This claim does not include the step of creation of the representation database.

Step (2): Identify the actual contribution

74 The contribution of claim 28 is the adding of a secure element to the pre-existing representation database using a bitwise logical OR operation.

75 The contribution of claim 29 is the updating of a pre-existing representation database to include an updated version of a secure element.

76 The examiner considered that the creation of the representation databases prior to the receipt of the data request was part of the contribution of the inventions claimed for claim 28 and claim 29 (as set down in the pre-hearing report dated 31 March 2022). Based on my construction of the claims discussed above, I disagree and consider that these claims only relate to operations carried out on an existing representation database

Step (3): Ask whether the contribution falls solely within the excluded subject matter?

Step (4): Check whether the contribution has a technical nature

---

[10] *See IPO decision BL O/044/15, Datanovation Ltd. Application, concerning patent application GB1208655.9,* Patent Ex Parte Decision O/044/15 (ipo.gov.uk)

77 Both methods are necessarily computer-implemented. They are confined to the computer on which they are implemented, so the *first AT&T signpost* is not met. Neither has any impact on the way the computer itself operates, so the *second, third & fourth AT&T signposts* are not met. The problem addressed is how to add or update elements in a representation database. This is a matter of administration and/or computer programming rather than a technical problem; hence, the *fifth AT&T signpost* is not met. I can see nothing in these methods which might be considered technical; I therefore find that neither method has a technical nature.

Potential for saving amendments

78 The dependent claims concern refinements to the representation database structure and the way in which queries are placed and additional data shared. I note the subject matter of claims 34 and 35 concern producing an irreversible representation database from which the original secure data cannot be backwards derived by decrypting. This process, although it would add to data security does not alter the analysis set out above and does not place the invention beyond those excluded under s.1(2)(c).

79 I have also carefully considered what has been disclosed by the application as a whole. I have found nothing in the application as filed which relates to a non-excluded invention, such that I consider there is no possibility of a saving amendment.

Conclusion

80 Taking all of the above into account, I find that the invention as claimed in application GB1705333.1 is excluded from patentability under section 1(2)(c) of the Act because it is a programme for a computer as such.

81 Having reviewed the application, I am unable to identify the possibility of a saving amendment.

82 As this patent application fails to meet the requirements of section 1(2)(c) of the Act, I therefore refuse it under section 18(3) of the Act.

Appeal

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

Dr L CULLEN
Deputy Director, acting for the Comptroller