F

Intellectual Property Office

BL O/961/22

04 November 2022

PATENTS ACT 1977

APPLICANT	Motorola Solutions Inc
ISSUE	Whether GB 1818409.3 complies with Section 1(2) of The Patents Act 1977
HEARING OFFICER	Peter Mason

DECISION

Introduction

1 Patent Application GB 1818409.3 is the national phase of a PCT application published as WO 2017/200403 claiming a priority date of 20th May 2016. It was subsequently republished as GB 2565011 on 30th January 20198. Despite several rounds of correspondence, the applicant has been unable to convince the Examiner that the application is allowable under Section 1(2) of the Act. As a consequence, the applicant was offered a hearing before a senior officer of the IPO and has requested that a decision be made on the papers.

The Application

2 The application is concerned with maintaining a chain of custody for assets uploaded to a central system. It is best illustrated by reference to Figure 1 of the specification.

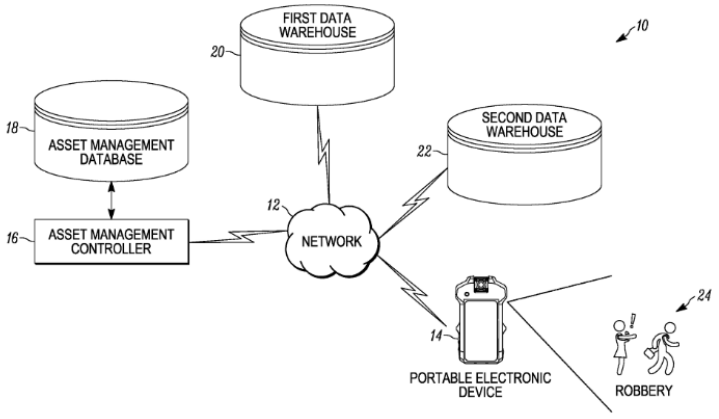

FIG. 1

3 The application is of particular use in law enforcement where a digital asset (24) i.e. an image of an event such as a robbery, needs to be uploaded from the portable electronic device (14) to a data warehouse (20 & 22). The application itself is concerned with checking or verifying whether the asset file in the data warehouse is the same as that on the portable electronic device (PED). On receiving the completion message from the PED, it retrieves and compares the details of the stored file and if they agree sends the PED a message confirming that they have permission to delete the asset from the device. This allows for the authenticity of the asset to be preserved according to appliable laws.

The Claims

4 This decision is based on the claims filed in amendment on 20th September 2021. It comprises two independent claims. Claim 1 directed to a system and Claim 8 to a method.

Claim 1 reads:

A system for maintaining a chain of custody for assets offloaded from a portable electronic device, the system comprising:

An asset management controller external to the portable electronic device, the asset management controller including:

a network interface;

an electronic processor coupled to the network interface configured to:

receive, from the portable electronic device via the network interface, an asset manifest including at least one asset identifier, at least one fixed-length unique identifier associated with the at least one asset identifier, and a manifest digital signature;

transmit, to the portable electronic device via the network interface, a storage message based on the asset manifest, the storage message identifying a data warehouse;

receive, from the portable electronic device via the network interface an upload completion message;

retrieve, from the data warehouse via the network interface, at least one asset file;

determine, for the at least one asset file, at least one asset file fixed-length unique identifier;

determine whether the at least one fixed-length unique identifier matches the at least one asset file fixed-length unique identifier, wherein the at least one fixed-length unique identifier is a hash of the at least one asset file;

determine whether the manifest digital signature is valid; and

transmit via the network interface, an asset deletion permission message when the at least one fixed-length unique identifier matches the at least one file fixed-length unique identifier, and the message digital signature is valid.

Claim 8 reads

A method for maintaining a chain of custody for assets offloaded from a portable; electronic device, the method comprising:

receiving by an electronic process external to the portable electronic device, via a network interface coupled to the electronic, from the portable electronic device, an asset manifest including at least one asset identifier, at least one fixed-length unique identifier associated with the at least one asset identifier, and a manifest digital signature;

transmitting, by the electronic processor via the network interface to the portable electronic device, a storage message based on the asset manifest, the storage message identifying a data warehouse;

receiving, by the electronic processor via the network interface, from the portable electronic device, an upload completion message;

retrieving, by the electronic processor via the network interface, at least one asset file from the data warehouse;

determining, by the electronic processor, for the at least one asset file, at least one asset file fixed-length unique identifier;

determining, by the electronic processor, whether the at least one fixed-length unique identifier matches the at least one asset file fixed-length unique identifier, wherein the at least one fixed-length unique identifier is a hash of the at least one asset file;

determining, by the electronic processor, whether the manifest digital signature is valid; and

transmitting, by the electronic processor via the network interface, an asset deletion permission message when the at least one fixed-length unique identifier matches the at least one

The Law

5 The section of the Act concerning inventions excluded from patentability is Section 1(2). This reads:

> "It is hereby declared that the following (among other things) are not inventions for the purposes of this Act, that is to say, anything which consists of –
>
> ...
>
> (c) **a scheme, rule or method for performing a mental act, playing a game or doing business or a program for a computer**;
>
> …

but the foregoing provision shall prevent anything from being treated as an invention for the purposes of this Act only to the extent that a patent or application for a patent relates to that thing as such."

6 In order to decide whether an invention relates to subject matter excluded by Section 1(2), the Court of Appeal has said that the issue must be decided by answering the question of whether the invention reveals a technical contribution to the state of the art. The Court of Appeal in *Aerotel/Macrossan*[1] set out the following four-step approach to help decide the issue:

1) Properly construe the claim;

2) Identify the actual (or alleged) contribution;

3) Ask whether it falls solely within the excluded subject matter;

4) Check whether the actual or alleged contribution is actually technical in nature.

7 The operation of the approach is explained at paragraphs 40-48 of the judgment. Paragraph 43 confirms that identification of the contribution is essentially a matter of determining what it is the inventor has really added to human knowledge, and involves looking at substance, not form. Paragraph 47 adds that a contribution which consists solely of excluded matter will not count as a technical contribution.

8 The case law on computer implemented inventions has been further elaborated in *AT&T/CVON*[2] which provided five helpful signposts to apply when considering whether a computer program makes a relevant technical contribution. In *HTC v Apple*[3], Lewison LJ reconsidered the fourth of these signposts and felt that it had been expressed too restrictively. The revised 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 make the computer a better computer in the sense of running more efficiently and effectively as a computer; and

---

[1] Aerotel Ltd v Telco Holdings Ltd (and others) and Macrossan's Application [2006] EWCA Civ 1371

[2] AT&T Knowledge Ventures LP and CVON Innovations Limited v Comptroller General of Patents [2009] EWHC 343

[3] HTC v Apple [2013] EWCA Civ 451

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

Analysis

9 The first step of the Aerotel test is to construe the claims. For the purposes of this decision, I will focus my attention on claim 1 as claim 8 is considered to be the same subject matter mutatis mutandis.

10 The claim presents little difficulty in understanding, but it would, I think be helpful, to make clear what several of the terms used mean. Helpfully, the specification at paragraph 13 provides ample information as to what is meant by an asset in this application. It is a multimedia file that may a video or audio recording or a digital photograph.

11 The electronic processor is an implementation of the asset controller (16, Fig 1). It is not too simplistic to say that this is a computer comprising as it does a processor, a memory and a network interface which are show in Fig 2. It is, as set out in paragraph 0017, connected to an asset management database which stores information about assets in a relational database.

12 Similarly, the specification makes clear what constitutes a “portable electronic device”. It gives a specific example of a body worn video camera manufactured by the applicant, but is could also encompass a handheld communication device, mobile telephone, a two way radio or a smart device.

13 I also believe it is essential to establish what is meant by “asset manifest”, “asset file fixed-length identifier” and manifest digital signature” given there are an intrinsic part of the process of issuing a “deletion permission message”.

14 An “asset manifest” is described in paragraph 24 of the specification as including at least an asset identifier and metadata. The asset identifier identifies the asset to be uploaded whilst metadata is date about the asset. The concept of metadata is well understood but by way of example in this application it may refer to the file type, size and a timestamp.

15 The fixed length identifier is discussed in paragraph 0037 of the specification. The example of a SHA-256 hash is given. Given SHA-256 converts an input text into a 256 bit output it will change with both length and content of the file. This provides a unique identifier for the file. This is of some relevance to the application as this is used to compare the uploaded file in the data warehouse and the file on the portable electronic device to ensure they are the same. Specifically, if the content and length of file are the same they will produce the same hash.

16 The term “digital signature” is readily understood and again the specification at paragraph 0037 is helpful. Here it describes the signature as one generated by signing the manifest with a private key on the portable ecteronic device using a public-private key encryption algorithm,

17 I also need to make clear how I understand the term “storage message”. I view this as a message containing the details of where the asset is stored in the data warehouse and the data storage path (0032).

18 It is here that I have an issue with the claim as it stands. There is a disconnect between the storage message and the update completion message. It would appear that there is a missing but implicit step of uploading (or offloading as the specification calls it) to the data warehouse using the information in the storage path.

19 Taking the above into account I believe the claim is a method of maintaining a chain of custody for assets “offloaded” from a portable electronic device to a data warehouse using an asset controller. The controller receives from the PED an asset manifest comprising an asset identifier and at least one fixed length file identifier such as a hash and a digital signature. A storage message is transferred to the PED and an asset is uploaded according to that message. On completion, the PED transmits an upload completion message. This is the key to the system as this is the trigger for the next part of the process. The controller compares for an asset identifier, the fixed length file identifier of the warehoused file with the identifier of the same asset identifier from the manifest of the asset on the PED. A determination is made if both the file length identifiers and the digital signature is valid agree the controller issues a deletion permission message to the PED.

20 The next step in the Aerotel test is to identify the actual or alleged contribution. From the correspondence the Examiner and the applicant are clearly in disagreement. For his part the examiner sees the contribution as relating to a computer program that:

> *-receive, from a portable electronic device via a network interface, an asset manifest including at least one asset identifier, at least one fixed-length unique identifier*
> *associated with the at least one asset identifier, and a manifest digital signature;*
> *-transmit, to the portable electronic device via the network interface, a storage message based on the asset manifest, the storage message identifying a data warehouse;*
> *receive, from the portable electronic device via the network interface, an upload*
> *completion message;*
> *-retrieve, from the data warehouse via the network interface, at least one asset file;*
> *-determine, for the at least one asset file, at least one asset file fixed-length unique*
> *identifier;*
> *-determine whether the at least one fixed-length unique identifier matches the at*
> *least one asset file fixed-length unique identifier, wherein the at least one fixed-length*
> *unique identifier is a hash of the at least one asset file;*
> *-determine whether the manifest digital signature is valid; and*
> *-transmit, via the network interface, an asset deletion permission message when*

the at least one fixed-length unique identifier matches the at least one asset file fixed-length
unique identifier, and the manifest digital signature is valid.

21 The attorney on the other hand sees the contribution as "*an improvement in the operation of the portable electronic device*" and in particular "*improved offloading of digital assets in a way that ensures a valid chain of custody*". They consider this a technical solution to a technical problem that is solved by the electronic processor (the controller) being made to operate in a new way.

22 Taking a view of both contributions offered, I am not sure that either are correct. Having arrived at the construction of the claim I have above, I consider that the Examiner's view is missing what may be the vital, albeit implied, step of "offloading the file". As to the attorney's view this is very broad and they offer no real assessment of the contribution.

23 What then is the contribution and does the step of "offloading the file" form part of it? The examiner has referred to the decision of the Hearing Officer in 0/135/22 which has many features in common with this application. It is also worth noting that in common with this application the attorney advanced similar arguments that the contribution lay in an improved PED (see paragraph 19 of that decision).

24 However, having read that decision, I am not so sure it offers me a path forward when considering this application. In particular, it was concerned with receiving an "offload" request and determining whether it should be allowed and creating a storage message. When viewed against this application it concerns only the transmission of the storage message to the PED in response to receiving the asset manifest. However, that is where it stops and it offers me no help or assistance in deciding on the further features of the claims.

25 In this application, the computing arrangement is what I would call standard. It is a fairly ubiquitous cloud arrangement with a controller. Taking this on board the contribution lies in the transmission and receipt of messages, the comparison of the messages and determination of whether a message indicating whether the asset can be deleted from the PED. It is, in short, a method of verifying an upload in a chain of custody for assets.

26 As such, I see the contribution as:

A system comprising a controller, the controller

receiving from a PED an asset manifest for an asset with an identifier, a fixed length indicator(PED) and a digital signature(PED);

transmitting a storage message to the PED indicating the data warehouse

(uploading the digital asset from the PED to the storage location in the message)

receiving from the PED an update completion message

the controller

retrieving the asset file from the data warehouse(W) and determining a fixed length identifier(W) for the asset

determining if the identifier(W) matches the indicator(PED)

determining if the digital signature is valid

and if the identifiers match and the signature is valid transmit a deletion permission message to the PED

27 The next step of the Aerotel test is to determine if whether this contribution lies in an excluded area.

28 The Examiner has suggested that the application falls foul of the business method exclusion. I can dispense with this issue at this at this point. I do not see this as a business method. It may have a specific application in a law enforcement environment, but I consider it to be a technical process and not one of a business or administrative procedure. It is about validating an uploaded file and that is not a business process.

29 That said, it clearly involves a computer program but is it one that is excluded as a result of the contribution falls entirely withing an excluded area such as a computer program?

30 The court in *Gemstar v Virgin* [2011] EWHC 3068 (CH) allowed one of the patents "the transfer patent" that were the subject of the litigation because it involved the transfer of a file. That is clearly the case here – a file is being transferred. This application though adds further steps to that basic file movement. In particular, it is a method of validating the transfer by verifying the accuracy of the transfer and then issuing a deletion permission message. To my mind, that goes beyond the basic scenario of "the transfer patent" of Gemstar.

31 In view of the message element of the claim, I need to give some consideration to the point raised by the attorney regarding *Protecting the Kids the World Over (PTKWO)* [2011] EWHC 2720 (Pat). There is a similar effect in play here insofar as there is a message being issued as a result of some analysis of several parameters. In the case of PKTWO that was an alarm message that was derived from an analysis of language used within communications to the computer. That alarm was considered to be allowable and in the words of Floyd J it "*solves a technical problem lying outside the computer, namely how to improve on the inappropriate communication alarm generation provided by the prior art.*

32 In this instance, the message produced is one that evaluates two conditions, the comparison of hashes and the digital signature, and issues a permission to delete message. It could be argued that this is only a message, but it is implicit that this will result in the asset being deleted at the PED. It solves the potential a problem of multiple or incorrectly uploaded assets in a system by providing an improved system that involves of validating the upload of a file before it is deleted.

33 The examiner in their report has referred to the decision in *Lantana* [2013] EWHC 2673 pointing out that the computing arrangement of the application is regarded as a system and that no effect is found outside it. That is clearly the case and I do not disagree. However, I am cognisant that Birss J cautioned in the same judgement at paragraph 17:

> *Simply because it is possible to construct a generalised category which includes both the claimed invention in this case and a previous decision in which a claim was held to be patentable, does not help. It shows that such things can be patentable in some cases but does not show that the invention in this case is patentable.*

34 I believe the point he was making is that it is the merits of each case that matter, and that you should not be drawn into the assumption that because an earlier case has similar facts they apply without consideration to the case in hand. There is not doubt that the cases are similar, but there is, I think a qualitative difference between them. Specifically, the current application performs a verification process that to my mind takes it beyond simply identifying and transferring of a file as was the case in Lantana.

Conclusion

35 For the reasons I have set out above, I consider that the application as set out in claims 1 and 8 is not excluded under Section 1(2) of the Act. Accordingly, I remit the application back to the examiner for further consideration.

36 In that regard, I make two observations:

- I have not considered novelty and or inventive step in this decision. I will not bind the examiner's hands in any way as regards these points. No doubt the results of any search will inform any decision as to whether any objections on these grounds will be forthcoming;

- Insofar as claim 3 and claim 10 are dependent on claim 1 and 8 respectively they fall within any analysis of the independent claims. I note that they appear to lack a causal connection with claim 1 and 8. Specifically, they relate to a re-validation message rather than a deletion permission message. Some consideration should therefore be given to whether this is a second invention.

Section 20 – Compliance Date

37 The current Section 20 date for this application is 23rd September 2022. Clearly, this has passed between the time the hearing was requested and my decision. In view of that, should the applicant wish to continue with the application they will need to file a Form 52 and the appropriate fee and I will exercise my discretion to allow it.

Peter Mason

Deputy Director, acting for the Comptroller