Intellectual Property Office

BL O/1000/22

15 November 2022

PATENTS ACT 1977

APPLICANT	Raytheon Systems Limited
ISSUE	Whether GB1906001.1 is excluded under Section 1(2)(c) of the Patents Act 1977
HEARING OFFICER	Peter Mason

DECISION

Introduction

1 Patent application GB1906001.1 was filed on 24th April 2019 and published as GB2583488 on 4th November 2020.

2 The patent application relates to a computer implemented application storage and distribution system which distributes applications, and the permissions associated with each application, to a user's mobile device in response to receiving their user credentials. Computing applications are programs or software designed to fulfil a particular purpose.

3 A search has not been performed under Section 17(5)(b). The examiner considered that the invention relates to subject-matter excluded from patentability under Section 1(2)(c) of the Patents Act 1977 ("the Act"), specifically to a program for a computer as such, and has maintained the objection under Section 1(2)(c) throughout the examination process.

4 The applicant has attempted to overcome this objection through argument and amendment filed on 28th June 2021 and with additional arguments in response to examination reports filed on 12th November 2021 and 24th February 2022, but has been unable to persuade the examiner that the invention has met the requirements of the Act and so the examiner invited the applicant to request a hearing.

5 The matter came before me on 23rd August 2022. The applicant was represented by Mr Alexander Rees who was instructed by Dentons UK and Middle East LLP. I am grateful for the skeleton arguments provided in advance of the hearing.

6 The only issue to be decided is whether the invention consists solely of a program for a computer, which the Act excludes from patentability under Section 1(2)(c).

The invention

7 The invention is a computer implemented application storage and distribution system which distributes applications, and the permissions associated with each application, to a mobile device of a user in response to receiving their user credentials. The application permissions include certificates signed by the developer, or known certificate authority, for validating the applications so that the applications can access the resources of the mobile device.

8 The application as filed states:

> *Paragraph 2: "Government and corporate organisations use mobile equipment that may be configured or modified for specialised operations that may not exist in the consumer domain. Current technological demands and in the current government and/or business environment means that those organisations that are adaptable to a changing environment are more likely to succeed than those that either require custom built technology or rely on old tried and tested technology. In particular, customising, modifying and building specialised mobile equipment is a time consuming, expensive and error prone process requiring many iterations before getting a stable workable solution."*
>
> *Paragraph 5: "There is a desire for an efficient, scalable, cost effective, safe and secure methodology for remotely provisioning mobile equipment with specialised functionality required by an organisation for each user/employee without sacrificing original equipment manufacturer safeguards and allowing said specialised functionality to be securely uploaded, installed and operated with minimum user input and/or technology experience. This can be used to maintain organisational or corporate policies at different sites, where certain functionality of the mobile equipment of a user may need to be temporarily disabled, turned off, removed or even enhanced e.g. geofencing policies in relation to technology capabilities."*
>
> *Paragraph 6: "A further desire is for using off-the-shelf or consumer mobile equipment with the aim to minimise customisation of the mobile equipment but at the same time provisioning the equipment with special functionality such as specialised applications that may require access to one or more, or all sensors, radio equipment, cameras and other hardware of the mobile equipment. There is also a desire to not fundamentally change or minimise changes to core functionality or OEM functionality of the mobile equipment. This would further maintain user familiarity of the user interface and keep the user experience stable whilst minimising circumvention of the default security of the equipment."*
>
> *Paragraph 7: "Furthermore, there is a desire to be able to easily replace such mobile equipment should they be lost or damaged in the field, where a user can requisition off-the-shelf or consumer mobile equipment and provision it in the field with the required special or specific functionality as the original lost or damaged mobile equipment. This can further minimise delays in meeting work demands but also reduces the engineering requirement by IT personnel and freeing up these resources to focus on updating, upgrading or designing further special or specific functionality rather than the time consuming and costly process of designing and provisioning new specialised mobile equipment."*

9 The invention provides a cloud-based distribution platform for providing a mobile device of a user with applications having required specific functionality associated with the user credentials of the user. The cloud-based distribution platform includes

an authorisation module to check user credentials and a certificate server to provide application permission data, in the form of certificates signed by a developer or known certificate authority, to accompany the distributed applications. The certificated applications can then access the restricted secure hardware or resources of the mobile device.

10 The latest claims were filed on 28th June 2021. There are two independent claims, claim 1 to a cloud-based distribution platform and claim 16 to a computer implemented method of provisioning a mobile device. The claims differ in form but are substantially the same and it was agreed during the hearing that they will stand or fall together. Claim 1 is set out below:

1. A cloud-based distribution platform for provisioning a mobile device of a user whilst in the field with required specific functionality associated with user credentials of the user, wherein the specific functionality was previously removed from the mobile device or the specific functionality was used by the user on another mobile device that the mobile device is replacing, the specific functionality comprising specialist operational functionality requiring access to restricted, secure hardware or resources of the mobile device based on fieldwork being performed by the user, the cloud-based distribution platform comprising:

an application storage medium configured for storing a plurality of applications, wherein a subset of the applications provide said specific functionality based on user credentials of a user, said specific functionality configured for using restricted, secure hardware or resources of a mobile device;

an authorisation module configured for, in response to receiving user credentials of the user from the mobile device, authorising distribution of the subset of applications with said specific functionality associated with the received user credentials of the user;

a preconfiguring module configured for, in response to receiving an identification of the mobile device, preparing and selecting applications for the subset of applications with said specific functionality associated with the received user credentials that are compatible with the mobile device based on the identification of the mobile device;

a certificate server configured for generating application permission data associated with each application in the subset with said specific functionality associated with the received user credentials, the issued application permission data including certificates signed by a developer or known certificate authority for validating, when said subset of applications are installed on the mobile device, said subset of applications to access said restricted, secure hardware or resources of the mobile device when executing said specific functionality; and

a distribution module configured to send the subset of applications and associated generated application permission data to the mobile device of the user for subsequent installation and execution on the mobile device to access said restricted, secure hardware or resources on the mobile device and provide said specific functionality to the user of the mobile device whilst in the field.

The law

11 The examiner has raised an objection that the invention is not patentable because it relates to one or more of the categories of subject-matter which are not considered to be inventions under the Act. This ‘excluded matter’ is set out in Section 1(2) of the Act:

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. [my emphasis]

The Court of Appeal's judgement in Symbian[1] tells us that in order to determine whether an invention falls solely within the any of the exclusions listed in section 1(2), the four-step test set out in its earlier judgement in Aerotel[2] must be used. The four steps are:

(1) properly construe the claim(s);

(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.

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. I shall consider whether the contribution is excluded alongside the question of whether the contribution is technical in nature, meaning I will consider the third and fourth steps of Aerotel together.

Argument and analysis

Step 1 - Properly construe the claim

12 The examiner and attorney agree that there is no difficulty in construing the claim in the light of the description.

Step 2 – Identify the actual (or alleged) contribution

13 Paragraph 43 of Aerotel suggests that the contribution can be assessed from the point of view of the problem to be solved, how the invention works and what the advantages are, stating "What has the inventor really added to human knowledge perhaps sums up the exercise".

---

[1] Symbian Ltd. v Comptroller-General of Patents [2008] EWCA Civ 1066
[2] Aerotel Ltd v Telco Holdings Ltd and Macrossan's Application [2006] EWCA Civ 1371

14 The application as filed indicates that the problem to be solved relates to the configuration of standard mobile equipment for specialised operations that may not exist in the consumer domain (paragraph 2). Paragraph 3 states:

> *"off the shelf consumer hardware may require bypassing the original equipment manufacturer restrictions using a process of rooting it, putting a new ROM on it and including applications with specialised functionality associated with the organisation's strategy or business". Paragraph 5 states "there is a desire to be able to easily replace mobile equipment should they be lost or damaged in the field, where a user can requisition off-the-shelf or consumer mobile equipment and provision it in the field with required special or specific functionality as the original lost or damaged mobile equipment".*

15 Paragraphs 11 and 102-107 of the application as filed, explain how the invention works. The remote deployment and administration of specialised and/or confidential applications based on a user's role may be achieved through a cloud-based application distribution system which is separate from the consumer application distribution systems provided by application platforms administered by the Operating System (OS) or the Original Equipment Manufacturer (OEM). The specialist or confidential applications can be installed in the mobile equipment without the requirement for rooting and/or fundamentally changing said mobile equipment; or overriding the standard security provided *if* the specialised or confidential application has accompanying application permission data, such as installation certificate(s), trusted root certificate(s) or public signature key(s). The application permission data provided with the specialised application is used by the mobile equipment to install and/or execute the specialised application(s) bypassing any OEM or OS device security controls. It was explained in the hearing that normally the application permission data or certificate is provided, either explicitly or implicitly, by the OS or OEM application platform.

16 The advantages of the invention are that specialised and/or confidential applications can be provided to mobile devices without rooting or fundamentally changing the mobile equipment to bypass existing OEM or OS device security controls. Rooting a device removes installation restrictions but also removes many built-in safeguards to the device's security.

17 The examiner summarised the contribution as: "The addition to human knowledge is an application storage and distribution system which distributes the appropriate applications to a user's device in response to receiving their user credentials, providing the advantage of allowing each end user to have a customised suite of secured and certificated applications on a standard hardware device, solving the problem of having to build custom devices or heavily modify existing devices for each user on a network."

18 The applicant considers this to be incomplete, and proposed the contribution to be: "The addition to human knowledge is an application storage and distribution system which distributes the appropriate applications and application permission data associated with each application to a user's device in response to receiving their user credentials, the application permission data including certificates signed by a developer or known certificate authority for validating the applications, when installed, to access restricted, secure hardware or resources of the mobile device,

providing the advantage of allowing each end-user to have a customised suite of secure and certificated applications on a standard hardware device, solving the problem of having to build custom devices or heavily modify existing devices for each user of a network while maintaining security of the standard hardware device."

19 I agree with the applicant that that the contribution includes the distribution of the applications with the application permission data, which includes certificates for validating the applications. I also agree that the contribution includes maintaining the security of the standard hardware device. I therefore determine the contribution to be:

An application storage and distribution system which distributes appropriate applications and application permission data, which includes certificates for validating the applications, to a user's device in response to receiving their user credentials, allowing each end user to have a customised suite of secured and certificated applications on a standard hardware device, without having to build custom devices or heavily modify existing devices for each user on a network, while maintaining the security of the standard hardware device.

Steps 3 & 4 - Ask whether it falls solely within the excluded subject-matter and check whether it is actually technical

20 The patent application as filed includes no technical details of the functioning of the data processing hardware and so it is clear that the contribution is put into effect by one or more computer program(s) running on conventional data processing hardware. Additionally there are no technical details relating to the user credentials, the method of authorising the user credentials, the certification method or how the certificates are distributed in association with the applications and so we can assume that there is no technical contribution provided by any of these aspects. It was confirmed in the hearing that the certification works in the same way as standard certification.

21 To assist in determining whether the contribution relates solely to a program for a computer, we use the signposts to technical contribution set out in AT&T/CVON[3] and by the Court of Appeal in HTC v Apple[4]. These 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;

[3] AT&T Knowledge Venture/CVON Innovations v Comptroller General of Patents [2009] EWHC 343 (Pat)
[4] HTC Europe Co Ltd v Apple Inc [2013] EWCA Civ 451

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

22 These signposts are useful guidelines only, providing a list of some of the factors that can assist in determining whether a contribution may be technical.

23 A network of computers is considered to be equivalent to a singular computer system, as in Lantana[5], and so the cloud-based distribution server and the standard mobile devices are considered to be equivalent to a single computer system. There is no technical effect on a process outside of this system, and therefore signpost (i) does not assist in identifying a technical contribution. The distribution of applications to mobile devices does not affect operations at the level of the architecture of any of the computing devices, and so signpost (ii) does not assist in identifying a technical contribution.

24 The applicant confirmed that they are not providing arguments in relation to signpost (i) and (ii) at this time, I see no reason to consider them further.

25 In relation to signpost (iii) the applicant argues that the installation of software applications from the cloud to the standard mobile user device allows the user device to operate in a new way, for example by changing frequencies of the user device for penetration testing or allowing access to the location data and or other sensitive data of the user device. The examiner stated that the computing devices are not operating in a new way (except in so far as any computing device running a new program operates in a new way) and the examiner considered that changes to permissions and parameters of the standard mobile device due to newly installed applications do not result in changes to the core operation of the computer in the standard mobile device itself. I find that while the mobile device provided with a new application program operates in a new way, the computer within the device does not. Signpost (iii) does not assist in identifying a technical contribution.

26 The examiner considered that signpost (iv) is not satisfied, stating that “your invention may cause a change in the way the user device ‘feels’ to the user, through alterations to applications or the security of programs running on it, but there is no change to the actual way that the device (either the cloud server or the mobile device) operates as a computer”. The applicant argued that signpost (iv) is satisfied as the computer runs more efficiently and effectively as a computer, stating that the advantage of allowing each end user to have a customised suite of secured and certificated applications on a standard hardware device solves one problem of having to build custom or heavily modified devices and solves another problem of maintaining the security of the standard hardware device. The applicant argues that the improved security of the user’s standard mobile devices, provided by not having to root the standard mobile devices to install the customised applications, corresponds to the invention making the computer a better and more effective computer as it is a more secure computer.

[5] *Lantana Ltd v The Comptroller General of Patents, Design and Trade Marks* [2014] EWCA Civ 1463

27 The applicant referred to Halliburton[6] paragraph 37, which was referenced in HTC v Apple paragraph 151, which states:

"The "better computer" cases—of which Symbian is paradigm example—have always been tricky however one approaches this area. The task the program is performing is defined in such a way that everything is going on inside the computer. The task being carried out does not represent something specific and external to the computer and so in a sense there is nothing else going on than the running of a computer program. But when the program solves a technical problem relating to the running of computers generally, one can see that there is scope for a patent. Making computers work better is not excluded by s 1(2)."

The applicant submitted that providing improved security is a technical problem relating to the running of computers generally and that a more secure computer is a computer which works better.

28 The applicant also referred to Gemstar[7] paragraph 42:

"It would be a relevant technical effect if the program made the computer a better computer in the sense of running more efficiently and effectively as a computer. That was the case in Symbian itself. This is described as a technical effect within the computer itself; it makes it a better computer, or solves a technical problem lying within the computer itself (see paragraph 54). It was also analysed as being the reasoning in Gale's Application [1991] RPC 305. On this analysis the present alleged invention fails. The computer program within it produces a technical effect within the computer in the sense that any functioning program does - the computer would not work in the same way without such effects. But those are not the effects referred to. More is required to avoid the exclusion, and (in this context) that "more" is something which makes the computer work better. The invention does not have this effect. It makes the computer, as a computer, work differently in the sense of processing data in a different way, but it does not make it work better, faster or differently in that sort of performance sense. The internal operation of the computer in this case therefore does not amount to a technical effect of the kind which I am considering in this section."

The applicant stated that security is a part of the performance of a computer, so that the providing of improved security may be regarded as providing a computer which works better and/or differently in a performative sense.

29 Finally, the applicant referred to paragraph 56 of Symbian[8]:

"Putting it another way, a computer with this program operates better than a similar prior art computer. To say "oh but that is only because it is a better program – the computer itself is unchanged" gives no credit to the practical reality of what is achieved by the program. As a matter of such reality there is more than just a "better program", there is a faster and more reliable computer."

The applicant submitted that the present invention is closely analogous to this conclusion as the effect is that it provides a mobile device having improved security, so that the mobile device and the overall system comprising the mobile device, may be regarded as a computer working with improved security.

---

[6] Halliburton Energy Services Inc's Patent Application [2011] EHWC 2508
[7] Gemstar – TV Guide International Inc v Virgin Media Ltd [2009] EWHC 3068 (Ch)
[8] Symbian v Comptroller General of Patents [2008] EWCA Civ 1066

30 During the hearing, it was clarified that the security of the standard mobile device after the installation of the secure and certificated specialised applications according to the invention was not improved over the security of the standard mobile device when updated with applications provided by conventional or commercial application distribution providers linked to the OS or OEM. Instead, the security of the standard mobile device of the invention was improved over the security of the standard device after rooting the mobile device to force the installation of the specialised applications.

31 The separate cloud-based application distribution system of the invention provides an alternative source of applications than commercial application distribution systems provided in relation to the OS or OEM. Additionally, the provision of the certificated specialised applications allows the installation of specialised applications on to a standard mobile user device, bypassing the OS or OEM restrictions of the mobile device, without the need to root the mobile user device. However, the computer system as a whole is not more secure than one using the commercial application distribution systems, and the standard mobile user device provisioned with specialised applications is not more secure than a standard mobile user device provisioned with applications from a commercial application distribution system. It appears clear that the computer system of the invention is not operating as a better computer. Signpost (iv) does not assist in identifying a technical contribution.

32 Finally, signpost (v) relates to the problem to be solved. The applicant submitted that the problem of having to build custom devices or heavily modify existing devices for each user on a network while maintaining security of the standard hardware device is overcome by the claimed invention and is not merely circumvented. The examiner considered that the problem concerns the organisation and distribution of specialised software and the claimed invention may have solved this problem, but the problem and solution are regarded as non-technical as it relates to a software matter.

33 I agree with the examiner that the claimed invention has overcome the stated problem and I also agree that the stated problem is not technical. The distribution of specialised software, provided alongside permission data to allow the installation into a standard mobile user device, appears administrative or organisational rather than technical.

34 None of the signposts point to a technical contribution. I therefore consider that the invention is excluded as a program for a computer.

35 For completeness. I confirm that I have also considered the dependent claims and the rest of the specification as filed. I have been unable to identify anything which would move the contribution beyond a computer program as such.

Conclusion

36 Having considered all of the arguments provide and all correspondence on file, I am of the view that the contribution made by the invention falls solely within the computer program exclusion.

37 I therefore find that the invention claimed in GB1906001.1 is excluded by Section 1(2)(c) as a program for a computer as such. I therefore refuse the application under Section 18(3).

Appeal

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

PETER MASON

Deputy Director, acting for the Comptroller