Case No:HP-2020-00036

IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
INTELLECTUAL PROPERTY LIST (ChD)
PATENTS COURT

Rolls Building
Fetter Lane
London, EC4A 1NL

26 June 2023

Before :

MISS CHARLOTTE MAY KC
(Sitting as a Deputy High Court Judge)
- - - - - - - - - - - - - - - - - - - -
Between:

ENSYGNIA IP LIMITED	**Claimant**
- and -	
(1) SHELL OIL PRODUCTS LIMITED	
(2) SHELL INTERATIONAL PETROLEUM COMPANY LIMITED	
(3) SHELL INFORMATION TECHNOLOGY BV	**Defendants**

- - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - -

Mr Martin Howe KC and Dr Geoffrey Pritchard (instructed by **Dehns LLP**) for the **Claimant**
Ms Lindsay Lane KC and Ms Beth Collett (instructed by **Norton Rose Fulbright LLP**) for the **Defendants**

Hearing dates: 30 January – 1 February 2023, 7 February 2023
- - - - - - - - - - - - - - - - - - - -

JUDGMENT

I direct that no official shorthand note shall be taken of this Judgment and that copies of this version as handed down may be treated as authentic.

Miss Charlotte May KC (sitting as a Deputy High Court Judge):

INTRODUCTION

1. By this action, the Claimant sues the Defendants for infringement of UK Patent GB 2 489 332 C2 (**the Patent**). The Defendants deny infringement and counterclaim for revocation on the basis that the Patent is anticipated and obvious over two pieces of prior art: US 7 379 912 B1 (**Kiliccote**) and EP 2 073 160 A1 (**Schmidt**), and that it is invalid for added matter, extension of protection and uncertainty insufficiency. The infringement allegation relates to claims 1 and 7; the validity attacks relate to claims 1, 2, 7 and 8 (although not all the attacks relate to all the claims).

2. In simplified terms, the Patent concerns a method (claims 1, 2) and a system (claims 7, 8) for identifying a user so that it can obtain access to a registered service. It involves the use of graphical encoded information or graphical object (for example in the form of a barcode or QR code) that is displayed on a display of a computing apparatus and scanned by the user's mobile device (such as a mobile phone). The information is either decoded by the mobile device (claims 1, 7) or by a server (claims 2, 8). Either way, the server establishes the identity of the user to determine if the user is registered, and if so, authorises the user to access the service.

3. The alleged infringement is a mobile payment system comprising a mobile phone app which can be used by registered customers at Shell petrol stations to purchase fuel. There are three iterations of the system that are relevant to infringement. The system comprises a number of sequential steps which I describe in more detail below. At this stage, it suffices to note that one of the steps requires the user to scan a QR code that is displayed on a piece of paper or card that has been attached on or near to the petrol pump.

4. The Patent was filed on 25 November 2010 (**the Filing Date**) and there is no earlier claim to priority. The Patent was amended post-grant under s.27 of the Patents Act 1977, and so it is the C specification that is relevant. There were amendments to both the description and the claims.

5. The amendments to the description include various statements that some of the embodiments and figures are "outside the scope of the claims". There is a dispute between the parties as to what impact those statements have on the construction of the Patent and whether, as a matter of law, the Patent should be construed without regard to those embodiments.

6. The amendments to the claims include introduction of the expression "obtaining a graphical encoded information item which is displayed on a display of a computing apparatus, <u>wherein the computing apparatus comprises the display and an electronic apparatus, and wherein the display is a sign.</u>" (with the underlined text added by amendment). The construction of this integer is at the heart of the case.

7. The Claimant contends that this integer relates to a "static" sign – that is, one which is not electronic <u>and</u> does not change between transactions. The Defendants contend that the integer relates to an electronic display on a computer screen or to a subset of a display akin to signage.

8. If the Defendants' construction of this integer is correct, the Claimant accepts that there is no infringement and that claims 1 and 7 of the Patent are anticipated by Schmidt. On the Defendants' construction, the issues of added matter, extension of protection and uncertainty insufficiency do not arise.

9. If the Claimant's construction of this integer is correct, the Defendants contend that the Patent is still anticipated and obvious over the prior art. In addition, they argue that it is invalid for added matter and extension of protection on the basis that, prior to amendment, the teaching and the claims were limited to a display on a computing apparatus and did not extend to a static sign. This depends on the proper construction of the application as filed and the B specification, to which I return below. Finally, the Defendants say that the Claimant's construction renders the scope of the Patent uncertain, with the result that it is invalid for insufficiency.

10. The Defendants also argue that, even if the Claimant's construction of this integer is correct, there is still no infringement because the claims require one message and one server, whereas the Shell system deploys two messages, and in the case of the second and third iteration, two servers.

CONDUCT OF THE TRIAL

11. The Claimant was represented by Mr Martin Howe KC leading Dr Geoffrey Pritchard and the Defendants were represented by Ms Lindsay Lane KC leading Ms Beth Collett. The trial was conducted live and there were no Covid issues. I had the benefit of written opening and closing skeleton arguments, as well as an oral opening and closing from both parties. I am grateful to counsel and their instructing solicitors for the work put into preparing their cases.

THE ISSUES

12. The issues are:

    i)   The identity of the skilled person.

    ii) The scope of the common general knowledge ("CGK"). Whilst formally there were two areas of disagreement, neither party relied on any of them to support its case on validity.

    iii) Construction.

    iv) Anticipation over both Schmidt and Kiliccote, although the attack over Kiliccote on either construction is limited to claims 1 and 7 because the Defendants accept that Kiliccote does not anticipate claims 2 and 8; and the attack over Schmidt on the Defendants' construction is limited to claims 2

and 8 because the Claimant accepts that claims 1 and 7 are anticipated on that construction.

v) Obviousness over both Schmidt and Kiliccote. In respect of Schmidt these attacks relate to claims 1 and 7 on the Claimant's construction, and claims 2 and 8 on both constructions. In respect of Kiliccote, these attacks relate to claims 1, 2, 7 and 8 on both constructions.

vi) Added matter, but only on the Claimant's construction.

vii) Extension of protection, but only on the Claimant's construction.

viii) Uncertainty insufficiency, but only on the Claimant's construction.

ix) Infringement, but only on the Claimant's construction and only in respect of claims 1 and 7.

THE WITNESSES

13. Each side called one expert. The Claimant's expert was Prof Keith Martin and the Defendants' expert was Dr Kevin Berisso. Neither side criticised the way in which the other side's expert gave oral evidence, and in my judgment they were right not to do so. I found both experts gave clear answers and did their best to assist the court on issues within their expertise. However, both sides criticised the way in which the other's expert had been instructed and/or prepared his evidence.

Prof Martin

14. Prof Martin is a Professor of Information Security at Royal Holloway, London. He has particular expertise in cryptography and its application to supporting cyber security in real world systems.

15. The Defendants made two criticisms of the way in which Prof Martin was instructed.

16. First, they criticised the fact that Prof Martin was given the original cited prior art before he was asked about the common general knowledge. This included two citations (referred to as Cobos and Trandal) which were dropped at some point before trial but which (I am told) were focused on cryptography. The Defendants pointed out that this approach was contrary to the established way in which an expert in a patent case should be instructed (at least where possible): the expert should generally discuss the CGK first, before being shown the prior art and then the patent in suit (see *Fisher & Paykel Healthcare Ltd v Flexicare Medical Ltd & Anr* [2020] EWHC 3282 (Pat) at [20]). They submitted that this misdirection caused Prof Martin to "start off on the wrong path", with CGK that was focused on the prior art and not on the field of the invention of the Patent. In particular, his first report included significant detail about cryptography even though he accepted in cross-examination that that there was no direct cryptographic interest in the Patent, but did not address barcodes and their uses.

17. The Claimant did not accept this criticism, arguing that there had to be a way of focussing the CGK and that the alternative of devising "bespoke" CGK relating to a more specific field or area that had been suggested by the instructing solicitors would be equally problematic.

18. I reject this argument, which did not justify why the Claimant had departed from the normal approach of sequential unmasking. Moreover, as Meade J made clear in *Fisher & Paykel* at [22], it is normally possible to direct initial discussions with an expert about CGK in a practical or workable way by describing the area of interest in general terms. That approach is preferable to showing the expert the prior art first.

19. However, as the Defendants accepted, even though Prof Martin addressed matters in the wrong order, in the end it did not seem to impact on the scope of CGK which was largely agreed between the parties. Whilst some points of CGK formally remained in dispute, as I explain further below, they did not have any impact on the substantive issues I have to decide.

20. Second, the Defendants criticised Prof Martin's approach to the prior art. This was because it became apparent during cross-examination that his written evidence was focussed on the claims of the prior art, and he had disregarded the disclosures in the description of both Kiliccote and Schmidt to the extent that they were different. Once this error was identified, he fairly accepted in cross-examination that certain relevant features were disclosed in the prior art even though he had maintained in chief that they were not.

21. The Defendants also argued that the combination of these two errors caused Prof Martin to take an approach to anticipation and obviousness that was too narrow and put him in an incorrect mindset that it was far too late to rectify in cross-examination. I do not think that there is any force to this submission, particularly bearing in mind what I have just said about the broad agreement on the CGK and the fact that Prof Martin changed his evidence about what the prior art disclosed once he understood the correct approach.

22. The Defendants also criticised what was said to be Prof Martin's apparent reluctance to put himself in the position of the skilled person implementing the prior art. This was in the context of questions put to Prof Martin about ways to implement various embodiments which were said to be obvious. The Claimant in turn criticised this line of questioning, saying that it was unsupported by evidence and was based on the ingenuity of counsel alone. These points are best dealt with in the context of obviousness, below.

Dr Berisso

23. Dr Berisso is an Associate Professor and Graduate Co-ordinator and Director of the Automatic Identification Lab at the University of Memphis, USA. His main area of research is AutoID and barcodes, and he has extensive experience in designing, developing and implementing AutoID systems. AutoID is short for automatic identification and data capture. The field pertains to someone who is specialist in designing barcodes and using them in systems.

24.   The Claimant criticised the way in which Dr Berisso had prepared his evidence in two respects.

25.   First, it was said that Dr Berisso had wrongly identified alleged CGK documents by way of extensive internet searching, with additional materials searched for and found by the Defendants' instructing solicitors. Two documents in particular were the subject of cross-examination, referred to as "the Gao paper" and "the Gumball Machine". The Claimant submitted that no proper consideration was given to whether these documents were CGK, and that this casts doubt about the reliability of Dr Berisso's evidence more generally. I do not think that there is anything in this criticism. This is because Dr Berisso did not suggest in his written evidence that the documents themselves were CGK (and he confirmed in cross-examination that they were not). Rather, they were intended to illustrate concepts which were said to be CGK, and which were largely agreed.

26.   Second, the Claimant criticised Dr Berisso's approach to the prior art, accusing him of picking integers out of the prior art without considering the proper context in which they arose, or the other factors required by the claims. This is said to undermine his evidence on obviousness, and so again is best dealt with in that context, below.

THE SKILLED PERSON

27.   There was no dispute between the parties as to the relevant law. The skilled person is someone who is likely to have a practical interest in the subject matter of the invention, which includes putting it into practice. I was reminded of the useful summary from Meade J in *Optis Cellular Technology Ltd v Apple Retail UK Ltd* [2021] EWHC 3121 (Pat) in which he said at [29]-[31]:

> "29.   I considered the applicable law recently in Alcon v. Actavis [2021] EWHC 1026 (Pat), drawing heavily on the decision of Birss J, as he then was, in *Illumina v. Latvia* [2021] EWHC 57 (Pat). The particularly relevant passages are [68]-[70] in *Illumina* and [31] in *Alcon*.
>
> 30.   At [68] in *Illumina* Birss J provided the following approach:
>
> > "68.   I conclude that in a case in which it is necessary to define the skilled person for the purposes of obviousness in a different way from the skilled person to whom the patent is addressed, the approach to take, bringing Schlumberger and Medimmune together, is:
> >
> > *i)*   To start by asking what problem does the invention aim to solve?
> >
> > ii)   That leads one in turn to consider what the established field which existed was, in which the problem in fact can be located.

iii) It is the notional person or team in that established field which is the relevant team making up the person skilled in the art."

31. And in *Alcon* at [31] I said:

"31. I intend to apply that approach. I take particular note of:

i) The requirements not to be unfair to the patentee by allowing an artificially narrow definition, or unfair to the public (and the defendant) by going so broad as to "dilute" the CGK. Thus, as Counsel for Alcon accepted, there is an element of value judgment in the assessment.

ii) The fact that I must consider the real situation at the priority date, and in particular what teams existed.

iii) The need to look for an 'established field', which might be a research field or a field of manufacture.

iv) The starting point is the identification of the problem that the invention aims to solve.""

28. This is not a *Schlumberger* type case, where the invention lies in the marriage of different technical fields, and so the skilled person to whom the Patent is addressed and the skilled person for the purposes of obviousness will be the same. Nevertheless, it is helpful to start by identifying the problem that the invention aims to solve, and the parties agreed that this can be done by reference to the Patent itself. They did not agree, however, on how to characterise or formulate that problem.

29. The Defendants submitted that the Patent states that the problem to be solved is preventing fraudulent activity by a so-called "man-in-the-middle attack", and that since this is done by the provision of a barcode or other graphical object, the problem is about how to use a barcode in order to provide an access or login methodology to enable provision of service to a user.

30. The Claimant criticised the Defendants' formulation, arguing that barcodes are part of the solution and not part of the problem. It submitted that the problem was to find enhanced security of identification or authentication of someone accessing a service.

31. In my judgment, the Claimant is correct on this issue. The invention is aimed at providing a secure means of identifying a user so that they can obtain access via a computing apparatus to a service that they are registered to use. This is clear from the section headed "Background to the Invention" at the start of the description which explains that the invention was made with a view to preventing different types of fraudulent activity, of which "man-in-the-middle attacks" are but one example (contrary to the Defendants' submission). It is also clear from the concluding section which states that "[t]*he invention provides a new and inventive way of providing secure access to services*" (p.26 line 8-9). This section of the Patent lists a number of perceived advantages of the invention, of which avoiding "man-in-the-middle attacks" is again only one. All the advantages relate

to improved security. Whilst the method and system of the Patent deploys a graphical encoded information item (of which a barcode is the exemplar), that does not mean that using barcodes is part of the problem that the invention aims to solve.

32. I am fortified in my view by what the experts said in cross-examination. Prof Martin said that the problem the Patent was trying to solve is improved access to services, either in terms of security or in terms of ease of use. Dr Berisso accepted that the problem was improving the security of identification or authentication when people access services via computing apparatus.

33. That leads on to the next issue, which is to ascertain if there was an established field at the time in which the problem existed, since it is the skilled person or team in that field which is the notional skilled person.

34. In opening, the Claimant argued that the skilled person was working in the field of information security, because that is Prof Martin's area of expertise and what he had said in chief. By contrast, the Defendants said that since the Patent specifically relates to the use of barcodes, the skilled person was a systems engineer within the field of AutoID. That was Dr Berisso's area of expertise and consistent with what he had said in chief.

35. However, in cross-examination, both experts changed their position somewhat. Prof Martin gave evidence that the field of AutoID and the wider field of information security have points of intersection. In particular, he said that the skilled person in the field of information security would recognise that barcodes could be used as a security technology and deployed for authentication and identification management purposes, but they would not have expertise in barcode symbology or the detailed algorithms required for decoding barcodes. Whilst he maintained the view that the Patent was addressing a security problem and fell within the area of information security, he accepted it also intersected with that part of the field of AutoID that related to the applications or uses of AutoID technology.

36. Dr Berisso's evidence was to the same effect. He agreed that the Patent was not aimed at someone who designs barcodes, any more than it was aimed at someone who was a specialist in cryptography. He accepted that it was directed towards someone involved in implementing systems who was an information security generalist, and that they could come from the AutoID field or the information security field.

37. The upshot of this evidence is that it does not matter whether the skilled person originates in the information security field or the AutoID field, as the problem that the Patent is aimed at sits at the intersection between them. This probably explains why, even though the experts came from these different fields, the parties largely agreed on the CGK, and the issues of validity and infringement did not depend on the few points that remained in dispute.

38. As a result of the evidence, by closing, both parties had refined their arguments on the identity of the skilled person. The Claimant submitted that the skilled person is a systems implementer who is an information security generalist. Whilst

the Defendants formally maintained their primary position that the skilled person was an AutoID systems engineer, the fall-back position was that it was someone who fell within the intersection. The Claimant's characterisation of the skilled person and the Defendants' fall-back position are effectively the same.

39.   In my judgment, the skilled person is a general information security professional who has an interest and experience in implementing computer related security systems. They will have gained that experience either working in AutoID or in the broader field of information security.

THE COMMON GENERAL KNOWLEDGE

40.   There was no dispute about the relevant principles. I was referred to *KCI Licensing Inc v Smith & Nephew plc* [2010] EWHC 1487 (Pat), [2010] FSR 31 at [105]-[112] (as approved by the Court of Appeal at [2010] EWCA Civ 1260, [2011] FSR 8 at [6]).

Agreed CGK

41.   An Agreed Statement of Common General Knowledge (ASCGK) was provided by the parties in advance of trial, for which I am grateful. I have reproduced that Statement below (subject only to minor edits to remove unnecessary detail).

42.   **Cryptography**. Cryptography provides a toolkit of mathematically based techniques for implementing core digital security services. These include **encryption**, which provides an ability to keep secrets and thus restrict who can make sense of data, **integrity**, which enables modification of data to be detected, and **authentication** (discussed below). Digital signature schemes, message authentication codes and hash functions all supported dataintegrity and were important components of authentication protocols.

43.   **Authentication and Identity Management**. These are critical features of a secure digital system and relate to the ways in which entities within a digital system are recognised and subsequently processed. Since the complex networks underpinning digital systems make it somewhat easy for devices to make connections, establishing what (or who) is attempting to make a network connection is a digital security challenge.

44.   Authentication is the process of establishing what (or who) is attempting to make a network connection.Identity management is the more general process wrapping around the way that identities(and authentication) is handled in a digital system. The most common authentication technique at the priority date was undoubtedly the password. Users would also have beenfamiliar with two-factor authentication techniques such as, for example, authenticating to an ATM by means of presentation of a card and entering of a secret PIN. Most UK bank users would have had chip-and-PIN and thus used cryptography without realising it when they made card payments. Biometric authentication technologies such as fingerprint readers and face recognition were available but in less use at the priority datethan today.

45. **Access Control**. Access control includes the process by which a computer determines who can have access to which data stored on the system. In most cases an authentication process must be undergone first before access control decisions are made (this broader decision-making process is sometimes referred to as authorization). Most access control techniques are part of a computer's operating system and general techniques such as access control lists, privileges and role-based access control would have formed part of the CGK.

46. **Network Security** refers to the principles and techniques used to protect computer networks, both wired and unwired. The CGK would have included an awareness that networks are typically modelled as a series of layers and that network security includes determining which security techniques to deploy at which network security layer. The CGK would have included awareness of protocols such as SSL/TLS, IPSec and SSH (for secure file download). The CGK would also have included awareness of security technologies used to support network protection such as firewalls (for inspection and control of traffic entering and leaving the network) and intrusion detection systems (fordetecting unwanted behaviour on the network). The CGK would have included a basic understanding of security deployed in common networking environments, such as wireless LANs (Wi-Fi) and the internet.

47. **Web Security** refers to security of activities on the world-wide-web. The CGK regarding web security would include consideration of risks created by weakness in thelanguages used to connect web traffic, issues relating to the ways that web addresses link to real web servers, and issues concerning privacy, including misuse of tracking data such as cookies. At the priority date both awareness and deployment of web security was not as high as today.

48. **Mobile Security** refers to security related to mobile telecommunications. The priority date falls in a transition period, when smartphones were becoming much more prevalent, and phones were increasingly being recognised as mobile computers capable of far more than just making calls. At the priority date the iPhone was only three-years old and so-called smartphones represented a minority of new mobile phone sales that year. The priority date represents a time when both the smartphone market and the uses that could be made of a smartphone were in flux. The CGK would have included an emerging awareness that all security issues previously considered for computers more generally (such as protection against computer viruses) increasingly also applied to smartphones due to their increased complexity and flexibility (such as the ability for uses to install their own applications on the phone – something unimaginable for older mobile phones). The CGK would also have included anawareness that this increased capability of smartphones also opened up the possibilitiesof them playing a role in the provision of security, such as supporting authentication for online banking.

49. **Automatic Identification and Data Capture**. AutoID refers to the process of identifying things (which could be persons or animals if using biometrics) automatically by the use of machine-readable technologies and automatically logging and/or processing the data without human involvement (i.e. other than via manual notation or keyboard input). The capability of AutoID to capture data and further process the data without error prone and slow human input is

important because it enables the attainment of accurate and reliable identification of physical representations in real time and in meaningful detail.

50.   AutoID technologies consist of three principal components:

i)   Data encoding – Encoding is the conversion of data (information) from one form to another. Typically, in AutoID, alphanumeric characters are translated into a form that can be read by a machine. For example, a part number or a URL may be converted into, or encoded into a bar code symbology, which is machine readable. The two predominant technologies used today are bar codes and RFID, described further below. Other technologies include biometrics, magnetic stripe (often seen on the back of bankcards), and smart cards.

ii)   Machine scanning and decoding – The machine scanner reads the encoded data and decodes it, meaning it converts the encoded data into another form of data. For example, in automatic identification, information or data may be converted from a machine-readable format back into a human readable format. For example, a part number or a URL that is in a bar code form (e.g. as a QR Code) may be converted or decoded into a human readable format (e.g. letters and numbers) by a bar code scanner.

iii)   Application – The decoded information is passed onto the application software (which may be on a server which may commonly include or interface with a database) which stores or processes the information received from the scanner.

51.   An example of elements that make up an AutoID system which carry out the components described above are shown below:
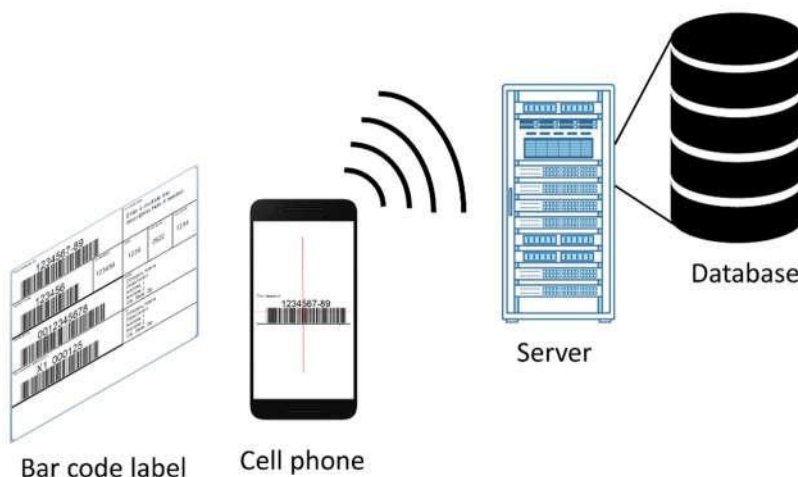
52.   As can be seen in this example, an object is labelled with a bar code which encodes information. The scanner is both capable of decoding and transmitting the information, either wirelessly (typically using Wi-Fi or cellular technologies)

or via a physical cable,to a server. The server may further process the information and/or store the informationin a database.

53.   A representative example is the use of bar codes on groceries. When the cashier scans the bar code on a grocery item at the checkout, the scanner transmits the item identifier (reference number for the grocery item) to the store's server, together with the scanner identifier. The computer looks for the price of the item that matches the identifier, sends that information back to the cash register associated with the scanner identifier, and the cash register then displays the price. At the same time, the computer alters the records in the database by reducing the number of that item in stock, resulting in real time inventory records of stocked items. The same can be implemented using an RFID tag (sometimes called transponders, to which information can be encoded) whose information can be decoded by a scanner which communicates wirelessly to the server/database. This process is impractical to replicate in terms of speed and accuracyby manual input.

54.   **Bar Codes**. Barcodes are a graphic representation of alphanumeric data. A barcode is typically limited in terms of capacity for storage and so generally contains just an identifier or reference number for the item it represents, which the computer can look up in databaserecords to retrieve further information, as illustrated in the grocery example above.

55.   Depending on the symbology in question, the data is either directly encoded with predetermined sets of bars and spaces representing individual characters or numbers (akin to how collections of dots and dashes represent letters in Morse Code) or mathematically generated values that represent collections of characters.

56.   Linear barcodes use the height of the barcode to make it easier to read the barcode since the barcode scanner (originally a laser that was passed across the barcode) does not technically need the height of the bar to be any taller than the diameter of the laser dot, and do not contain differing information in the vertical direction.

57.   Matrix symbologies are also generally called barcodes, but technically do not use bars in the same sense as the previously discussed types of barcodes. Unlike linear barcodes, matrix symbologies need to be scanned with a camera (imaging) system because of theirtwo-dimensional nature. The QR Code is a matrix symbology.

58.   In general, encoding data in a matrix symbology is significantly more difficult than encoding information in linear or stacked symbologies. There is more to the process than matching the characters to the bit patterns due to the logic that occurs behind the scenes to help with the space efficiency of the symbology.

59.   **Use of Mobile Phones as Bar Code Imagers**. Mobile phones with camera functionality that can also double up as bar scanners were CGK as at the Filing Date. The mobile phone can either process the decoded information or transmit the image to a server (either by using cellular communication means or Wi-Fi) which can then decode the image or display the matrix code.

60.   The mobile phone with a digital camera (being an imager) has an on-board computer that will process the image and attempt to find and decode any barcode that it "sees". The major advantage of imagers is their ability to scan from different

directions, whereas other scanners need to be held in a particular direction for scanning.

61.   For mobile phones without camera functionality, there were various applications available for download (often for free) for both Apple and Android phones that would decode bar codes (e.g. ZXing crossing app, RedLaser, the "bar code scanner" app) and then selectively open the web browser, the contact manager software, or sometimes just a notepad.

62.   Such scanning functions of a mobile phone including with the use of QR Codes was a commonly accepted process as at the Filing Date, at least by the Skilled Person.

63.   **Bar Code Carriers**. The use of mobile phones for the displaying of barcodes was well known. In addition to displaying a barcode on a mobile phone, the Skilled Person would be familiar with displaying barcodes on any number of devices and media. Commonly used media would include anything from physical paper labels, posters, it could be printed on the item itself, and on billboards, etc. (see for example a movie advert on a billboard).

64.   It should be noted that anything, including a barcode, that could be displayed on a traditional computer monitor could be displayed on any other sort of electronic display.

65.   The Skilled Person would understand and appreciate that the computer controlled screens that would be used to display barcodes could be of many different types, including tablet screens, mobile device screens (mobile phones), electronic or digital billboards (for outdoor use), smaller electronic or digital poster/banner sized signs for indoor venues (e.g. concert halls, airports, etc.), or even smaller displays near doors to indicate schedules or other access related information. The Skilled Person would understand that the screens could be of a number of differing technologies such as e-paper (e.g. Kindle screens), LEDs, LCDs, or any other available technology. Basically, any display technology that provides a resolution sufficient to display a picture could also display barcodes.

66.   **Radio Frequency Identification**. As explained above, alongside barcodes, RFID is one of the most widely used machine-readable technologies that are included in the AutoID "umbrella" of technologies. RFID uses radio waves to transmit data between the RFID tag and an RFID reader.

67.   Typically, an RFID system consists of transponders, readers, and a server/database. Like barcodes, information, for example, identifiers such as serial numbers, expiration codes, reference numbers can be encoded by programming into a transponder. A transponder is essentially a microprocessor chip consisting of an integrated circuit with memory. Active transponders have an on-board power supply which enables active transmission of information on a persistent basis, whereas passive transponders only transmit when interrogated by the reader. Passive transponders can operate without power as they can absorb the radio energy from the reader to generate the power needed to transmit radio signals. There are also battery assisted passive transponders which come with a battery to enhance the read range. In addition, transponders may operate in

different frequencies. The information in the transponders can only be decoded by compatible readers (sometimes called interrogators) which use the correct frequency and protocols to read the transponders. Transponders with different attributes have different characteristics such as the length ofthe read range, which is chosen depending on the application.

68. In general, to the Skilled Person, barcodes and RFID are very similar technologies, and often used interchangeably.

69. **Application**. As explained above, the final component of AutoID technologies is the application software, which typically includes a client application in communication with a server which may commonly include or interface with a database. Such software was part of the CGK as at the Filing Date.

70. The client application can be run on anything with a computer (e.g. a desktop computer or mobile device).

71. Desktop computers running an application would include a user interface with a field where a piece of information needed be inputted, and a scanner wired to the desktop. When the user scans the barcode the information in the barcode would be decoded by the barcode scanner and input into the relevant field.

72. As described above, mobile phones were capable of scanning barcodes at the Filing Date and were further capable of decoding barcodes and running client applications that used scanned barcodes. Mobile phones could be configured to merely decode the barcode (if in communication with a server, see further below), but for the most part, mobile phone applications were configured to decode the barcode and use the decodedinformation for a subsequent function.

73. **Common Use Cases for Bar Codes**. The parties agreed that the following use cases were part of the CGK.

    (i) Identification of part numbers (for example, most car parts will have them), traded goods (for example, items sold in grocery stores), and pallets in warehouses

74. This is done by affixing the barcode, via a label or direct marking, on the items. Typically, retail purchasers can use the identifiers to look up the price when checking out and/or for allowing the retailer (or potentially the consumer) to look up additional information about the item being purchased. In cases where the price is being queried, the barcode is scanned and then the value is looked up in a database with the current prices. For the case where the part number is being queried for additional information, the querying device (mobile phone, computer, etc.) would place the part number in the search field, relieving the user of having to type the information in by hand, before executing the search.

    (ii) Identification of persons (using unique identifiers such as a membership number)

15

75.   A typical use case where specified persons need to be identified is in access control where access to a particular building or room might need to be managed to ensure only authorised persons gain access to certain rooms.

76.   In applications directed to the identification of persons/users, a person with a pass/identification badge with a printed barcode which encodes the individual's unique identifier ("UID") would place the pass/badge under the barcode scanner (or possibly swipe the barcode through the scanner). The barcode scanner would be fixed at the door of the relevant room, capable of reading barcodes that are held within a few inches of the scanner. The scanner would then send the UID, together with the reader ID/location ID to a computer server, which looks up the database to determine if the holder of the pass/badge (identified by the UID) has authorization into that room (identified by the reader ID). If the database establishes that the person with that pass is authorised to access the relevant room, the server would then send a signal to the electronic lock associated with the door to the room, remotely and electronically unlocking the lock. If greater security was required, the person may well need to have a PIN or secondary security token in addition to the barcode ID card.

77.   Typically, the entire facility or building would use one database which holds all of the UIDs and levels of access authorised for each UID since any given person's list of room authorization may be different from another person. The database may also record all attempts, including failures and access denied attempts. CGK examples used bar codes or RFID.

78.   Similar principles have been used in ticketing in airports, trains or events. In the case of use by airlines, the information in a boarding pass (whether in paper form or displayed on a mobile phone) includes the ticket holder's name, flight, class of service, and other information of importance to the airlines.

(iii) Identification of location (barcode labelled storage locations in warehouses)

79.   AutoID has been used to keep an inventory of items and where each item is stored, typically in a large warehouse, or a number of warehouses. Each storage location is labelled with a unique barcode which then serves as a location identifier. The database would record relevant information, such as the description of the items in a location (for example, spanners of particular size) together with the unique identifier of the item (for example, UPC number) and the location ID, together with the number of items stored. A worker working in the warehouse could then scan the location and the item every time the item is being stored or retrieved so that the database can keep track of the volumes of the different items that can be located in each labelled location. A custom application would be used to enable the worker to update that "x" number of items were added to, or removed, as the case may be, from location "y". In some instances additional logic could be added to the software and the location barcodes, such as adding an extra character (for example, "L" to indicate location) as a simple form of error checking to ensure that the person using the system is scanning the location and not the item.

(iv) Unique identification of items/Serialization (serial number of an individual item)

80.   Serialized barcode references are primarily used at the manufacturing level to help with the identification of individual components or finished products that have had testing done on them. The manufacturer's manufacturing systems would log the serial number and the test results to a database so that the company could prove that the product was successfully tested before shipment.

(v) Identification of characteristics of items (batch numbers, expiration dates)

81.   Barcode references can be used to indicate batch/lot information, which is information that indicates the specific grouping of items which were produced in the same timeframe. Batch/lot information can be used for tracing back items which are claimed to be faulty and identify all other similarly produced items which may have the same fault and so need to be recalled.

82.   Another example of attribute data would be the expiry information (the date at which an item's useful life was determined), which is often used in warehousing operations, allowing the warehouse systems to determine which items are close to expiry and taking appropriate action, for example, preventing shipment.

(v) Tracking/tracing moving items

83.   Barcodes can be used to track moving items such as mail, parcels, and luggage. In the case of mail and parcels, the bar codes on them are scanned to enable automatic sorting and thereafter, scanned when they reach the delivery point. Because the scanner at the delivery point will communicate its scanner ID/location ID together with the item ID, the database can then maintain a record of whether the item has reached the delivery point. A similar principle is used to track the whereabouts of items in a supply chain.

84.   In the case of airline luggage, a barcode might be affixed so that it can be scanned when it is being loaded on the aircraft. As with the postal service, the scanner will transmit the luggage ID together with the scanner ID so that the database can record which luggage with luggage ID has been loaded on which aircraft.

85.   The associated passenger will also have been given a boarding pass with a barcode, which is linked to the luggage ID. The scanning of the boarding pass is recorded at the gate because the scanner at the gate will send the boarding pass ID together with the scanner ID to the database. Because the boarding pass ID and the luggage ID are linked, the database is able to verify that there is no baggage on board that does not have an associated passenger in the aircraft. If a passenger fails to board on time, the relevant luggage can be easily identified and removed.

Disputed CGK

86.   There was an agreed list of disputed CGK included at the end of the ASCGK, but by closing, this had narrowed to two outstanding points: (i) applications using barcodes and (ii) barcode use cases. Neither party framed its case on validity by reference to these points specifically, which would tend to suggest that they do not need to be resolved. However, the Defendants argued that they were still relevant since the first point demonstrates the degree of knowledge that the skilled person has about implementing systems; and the second point provides the

framework against which the Patent should be assessed and may also shed light on the extent to which the skilled person would consider the use of different barcode carriers such as digital displays, posters and other materials. Whilst the two points were presented separately (at least by the Defendants in argument), they are overlapping issues and I find it more convenient to address them together, particularly in light of how the evidence came out.

87.   The Claimant accepted in closing that it was CGK to use a mobile phone as a scanner in respect of the following use cases:

 i) reading a symbol on the wrapping of fast-food items and getting nutritional value on the screen;

 ii) reading a symbol in an advertisement and having the phone act as a web-browser that is automatically directed to the advertising company's website;

 iii) reading a symbol that will automatically download a particular ringtone, screen "wallpaper" or purchased music into the phone;

 iv) reading a symbol that is part of a game or contest, and links the user to the contest operator;

 v) reading a symbol in an advertisement and then being automatically connected (by voice or data) to a local distributor of the item or service, for example via a webpage or embedded data in a virtual business card.

88.   This list comes from "The Bar Code Book" by Roger C. Palmer, dated 2007, and it is clear in context that the reference to "symbol" includes a barcode.

89.   Prof Martin also accepted in cross-examination that the skilled person would know of the following uses, at least at a high level (but not necessarily with sufficient knowledge to build a complete system):

 i) Using an application on a mobile phone to communicate with a server to access or update information stored on the server. That could include, for example, use of a database within the server for login authentication of users before they can access functionalities within the application. In this context, the skilled person would know that storing information on a server avoids using the more limited memory space on the mobile phone, and that decoding at the server saves on application processing power. They would also know about basic server security issues and protocols as they relate to webservices.

 ii) Using a mobile phone to read or scan a QR code to access information (such as contact information, which can be scanned from a QR code and sent directly to the phone's address book, or information from a website).

 iii) Using a mobile phone to read or scan a QR code to buy items online (for example via an advertisement or in store, when scanning the code takes the user directly to the mobile website or online version of the store). This

included the use of 2D barcode solutions where the mobile acted as the point of sale device and facilitates payment transactions.

iv) Mobile payment functionality, including using QR codes for mobile payment. In this context, the skilled person would have awareness of PayPal and other payment APIs.

90. It follows that all of what is set out in the preceding paragraph is also CGK, and I so hold.

91. However, the Claimant did not accept that the content of the Gao paper and the disclosure of the Gumball Machine were CGK. As noted above, the Defendants did not suggest that they were either, so I do not need to address these materials further.

THE PATENT

92. The Patent starts by identifying the field of the invention which (as noted above) is said to relate to the handling of encoded information. The next section is headed "Background to the Invention", where it states:

> Identity cloning is an increasingly common phenomenon. Fraudsters use a wide variety of mechanisms to in order to illegally elicit personal information such as usernames, passwords, dates of birth and addresses with a view to cloning identities. One such mechanism is where a fraudster provides a spoof (or clone) of a website, which to an unsuspecting user appears identical to the original. Believing that the website is the original, the user provides personal information, such as login details or credit card details, which are recorded by the fraudster. A more sophisticated approach is a "man-in-the-middle attack" in which a fraudster provides the clone website and records the personal information, but also passes the personal information to the real website, which logs the user in as normal. In this way, the user does not notice anything different and the fraudster is able to obtain the personal information without alerting the user. This invention was made with a view to preventing these and other similar types of fraudulent activity.

93. There then follows a section headed "Summary of the Invention" which is made up of the consistory clauses. Three figures are then described in the next section, headed "Brief Description of the Figures". Figure 1 is a schematic illustration of a system in which embodiments of the invention can be implemented. Figure 2 is a schematic illustration of a method according to embodiments outside the scope of the claims. Figure 3 is a schematic diagram illustration of a system and method according to alternative embodiments. Whilst it does not say so here, the reader later learns that Figure 3 is also outside the scope of the claims.

94. The last section of the description is headed "Detailed Description of Embodiments of the Invention". This comprises the bulk of the specification, running to over 20 pages (out of a total of 28), with a detailed description of each of Figures 1-3 and then a description of three different embodiments. As with the figures, all but one of the embodiments are said to be outside the scope of the claims.
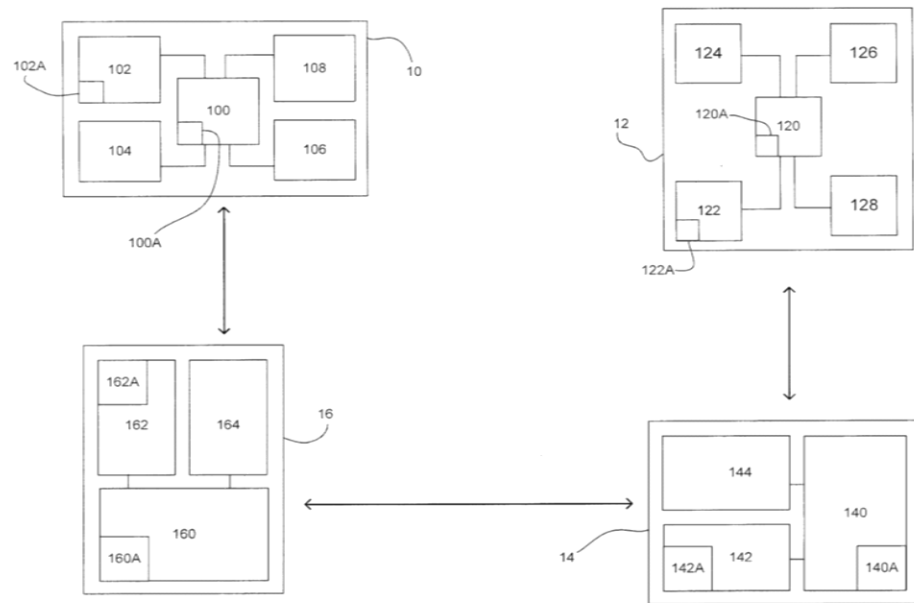
95. Figure 1 is reproduced below.

Figure 1

96. The system comprises computing apparatus 10, a mobile device 12, first server apparatus 14 and second server apparatus 16. The servers may be located in the cloud. The mobile and the first server communicate wirelessly with each other. The mobile device comprises the means 124 (such as a camera) for obtaining encoded information items which are external to it.

97. The first server also communicates with the second server in any suitable manner. The computing apparatus is configured to receive signals from the second server, to interpret information contained therein and to display the information on a display 104 for consumption by the user. The computing apparatus may also comprise a user interface 108, such as a mouse, touch pad or keypad via which user input can be received. It also comprises a controller 100, which is operable under the control of the computer-readable code to control the other components, such as the display.

98. Figure 2 is reproduced below. As noted above, it illustrates a method according to a first embodiment that is expressly stated to be outside the scope of the claims.
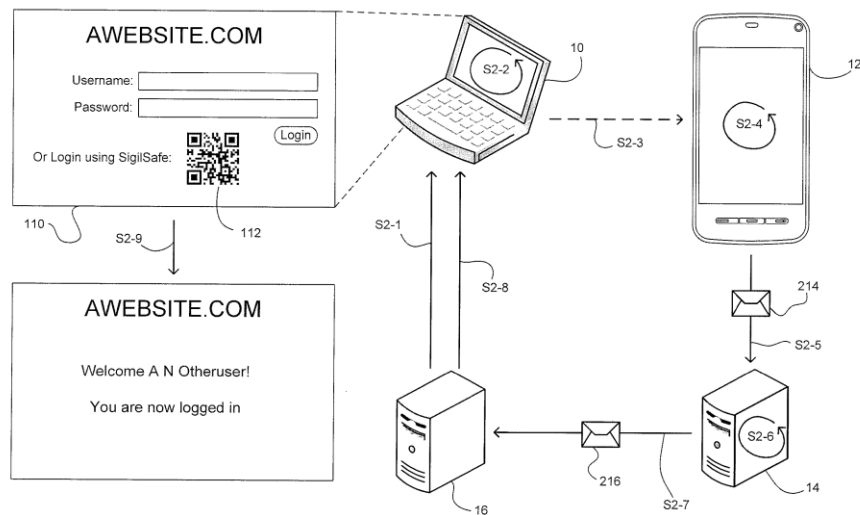
Figure 2

99. The method is described by reference to nine steps, S2-1 to S2-9.

100. In this configuration the second server provides the computing apparatus with information (eg web page information), possibly in response to a request received from the computing apparatus after user input (S2-1). The computer displays a webpage containing an encoded information item 112, which may be a barcode or QR code or other graphical object ("GO") (S2-2). The GO contains encoded information *inter alia* identifying the computer on which it is displayed. It may also comprise information identifying the first server and the second server, and verification information items for allowing verification of the GO to ensure that it is not a fraud. The GO is read by the mobile device (S2-3) and decoded by an application on the mobile device (S2-4). The mobile device then sends a message to the backend server (the "first server") (S2-5). The message contains the decoded information and information which identifies the device or the user that will have been provided in advance as part of the registration process that is required to allow the user access to the service provided by the first server.

101. If the user/device is properly authorised (S2-6), the first server sends a message to a second server apparatus (S2-7). The message comprises the identity of the user and confirms that the user is authorised to access the services of the second server. The second server is a web server, and it provides service to the user, namely logging him/her into the computer (S2-8). The server sends a signal to indicate this to the computing apparatus, and the computing apparatus displays this received information to indicate that the user is logged on (S2-9).

102. There are also various optional features which are aimed at improving security, such as checking that the computing apparatus is in direct contact with the second server and not a proxy server, checking that the GO is genuine, and requiring the user to provide a username and password to log into the webpage.

103. Figure 3 depicts a similar system to Figure 2, save that it only comprises the first server apparatus (which is a web server apparatus). The Patent provides that Figure 3 is also outside the scope of the claims.

104. In addition to the figures, the Patent then goes on to describe further embodiments. These are introduced by the following text:

> It will be understood that the invention may be implemented within systems other than those described above. Such implementations are described in brief below. Although these are described briefly, it will be understood that the operations may be substantially the same as those described above and may include the [*sic*] some or all of the same steps and features.

105. Three embodiments then follow: the building security embodiment, the ATM embodiment and the self-service shopping embodiment. The latter two are said to be outside the scope of the claims, and so the focus at trial was on the first.

106. The building security embodiment is exemplified by reference to an electronic door lock. Upon approaching the door, the user uses their mobile phone to scan the GO (or other encoded information). The first message (an entry request) is sent to the first server. This message includes the encoded information and means to identify the user or device. Once the appropriate identity is confirmed, the server transmits a signal to the electronic door lock (either directly or via the second server if there is one), authorising it to open.

107. The issue is where and how the GO or other encoded information is displayed. This is addressed in the description in the context of this embodiment as follows:

> In such an embodiment, the computing apparatus 10 may comprise an electronic door lock. The encoded information item 112, 312, such as a GO as described above, may be displayed on a sign geographically proximate to the electronic door lock. In embodiments outside the scope of the claims, the GO 112, 312 may be provided on an electronic display geographically proximate to the electronic door lock. In such embodiments, the encoded information item may be periodically updated following receipt of signals from the first server apparatus 14.

108. This passage is central to the issues on construction, and so I return to it in that context below.

109. For completeness, and even though they are outside the scope of the claims, it is worth noting some of the disclosure about the other embodiments.

110. In particular, as regards the ATM embodiment, the encoded information item is produced in response to the user's request for cash withdrawal. It follows that, with this embodiment, the encoded information item will change from one user to the next. The encoded information item is displayed by the ATM. There was no dispute on the evidence that an ATM has an electronic display in the form of a screen, and so it follows that the encoded information item is provided on an electronic display with this embodiment.

111. As regards the self-service embodiment, the encoded information is "provided on a smart tag of a product for sale" (p.24 line 7-8). The smart tag is the computer apparatus for this purpose. The point of using the smart tag is so that it can be automatically disabled (by receipt of a signal from the second server) once the

product has been paid for. The Patent does not say how the encoded information is displayed.

112. Following a description of the three specific embodiments, in the final pages the Patent reverts to more general teaching. Of note, it provides that in some embodiments the encoded information may be changed periodically. It also teaches that instead of decoding by the mobile device before sending the first message, the encoded information may be transmitted in the first message for decoding by the first server apparatus.

113. Finally, the Patent sets out several perceived advantages to the invention. These can be summarised as follows:

    i)   The provision of encoded information reduces the possibility of a "man-in-the-middle attack". The description states that "*[t]he invention is particularly effective in this respect in embodiments in which the computer program code for generating the encoded information item is stored on the computer apparatus 10 and is configured such that the encoded information item is only provided (i.e. displayed, emitted, output etc.) when direct communication with an application running on the web server 14; 16 is established*". It goes on to explain that this is because, if there is a proxy server between the computing apparatus and one of the servers, the encoded information cannot be provided to the computing apparatus, the user will not be able to access the service and sensitive information will not thereby be divulged.

    ii)   If the system employs the optional means of verifying the encoded information item (which can be achieved by a verification item that is changed periodically), this reduces the chances of fraudsters cloning the encoded information item and the service.

    iii) The provision of encoded information also reduces the amount of personal information (e.g. usernames and passwords) that are required to access the service, the security of which may be compromised.

    iv)   However, if a username and/or password is required in addition to the encoded information item, this can add an extra layer of security and/or tiered strengths of authentication.

    v)   The invention also provides for a faster log-in process.

    vi)   Security advantages are also achieved by using a device (such as a mobile) to establish communication with the server and the identity of the user which is separate from the computing apparatus that is then used to access the service from the server. This is said to take the authentication process "out of band" and adds security because it is more difficult for a fraudster to detect, intercept or compromise multiple communication channels or bands.

CONSTRUCTION

General principles of construction

114. Save for one point considered below, there was no dispute as to the relevant principles. The parties referred me to *Saab Seaeye Ltd v Atlas Elektronik GmbH* [2017] EWCA Civ 2175 at [18], citing *Virgin Atlantic v Premium Aircraft* [2010] RPC 8 at [5] which summarises the main principles of construction. These are:

> "(i) The first overarching principle is that contained in Article 69 of the European Patent Convention.
>
> (ii) Article 69 says that the extent of protection is determined by the claims. It goes on to say that the description and drawings shall be used to interpret the claims. In short the claims are to be construed in context.
>
> (iii) It follows that the claims are to be construed purposively – the inventor's purpose being ascertained from the description and drawings.
>
> (iv) It further follows that the claims must not be construed as if they stood alone – the drawings and description only being used to resolve any ambiguity. Purpose is vital to the construction of claims.
>
> (v) When ascertaining the inventor's purpose, it must be remembered that he may have several purposes depending on the level of generality of his invention. Typically, for instance, an inventor may have one, generally more than one, specific embodiment as well as a generalised concept. But there is no presumption that the patentee necessarily intended the widest possible meaning consistent with his purpose be given to the words that he used: purpose and meaning are different.
>
> (vi) Thus purpose is not the be-all and end-all. One is still at the end of the day concerned with the meaning of the language used. Hence the other extreme of the Protocol – a mere guideline – is also ruled out by Article 69 itself. It is the terms of the claims which delineate the patentee's territory.
>
> (vii) It follows that if the patentee has included what is obviously a deliberate limitation in his claims, it must have a meaning. One cannot disregard obviously intentional elements.
>
> (viii) It also follows that where a patentee has used a word or phrase which, acontextually, might have a particular meaning (narrow or wide) it does not necessarily have that meaning in context.
>
> (ix) It further follows that there is no general 'doctrine of equivalents.'
>
> (x) On the other hand purposive construction can lead to the conclusion that a technically trivial or minor difference between an

element of a claim and the corresponding element of the alleged infringement nonetheless falls within the meaning of the element when read purposively. This is not because there is a doctrine of equivalents: it is because that is the fair way to read the claim in context.

(xi)   Finally purposive construction leads one to eschew the kind of meticulous verbal analysis which lawyers are too often tempted by their training to indulge."

115.   As Arnold L.J. recently made clear in *InterDigital Technology Corporation & Ors v Lenovo Group Ltd & Ors* [2023] EWCA Civ 105 at [81], the three key considerations are the wording of the relevant integer of the claim, the context provided by the specification and the inventor's purpose.

116.   The Defendants' counsel also reminded me of the statements in two recent judgments from Meade J. to the effect that a patentee is likely to have a generalised concept in mind for his or her invention and the claims are not presumed to be limited to the preferred embodiment(s), particularly if general language is used in the claims. See *Add 2 Research and Development Ltd v Dspace Digital Signal Processing & Control Engineering GmbH Dspace Ltd* [2021] EWHC 1630 (Pat) at [92] and *Promptu Systems Corp v Sky UK Ltd* [2021] EWHC 2021 (Pat) at [130].

117.   The point of law in dispute related to the embodiments expressly stated to be outside the scope of the claim.

118.   The Claimant argued that it is trite law that the claims must be construed by reference to the Patent as a whole, including those parts of the specification which relate to an embodiment (or parts of an embodiment) that are no longer claimed. In this regard, I was referred to *Wood v Capita Insurance Services Ltd* [2017] 2 WLR 1095 at [10] where Lord Hodge said:

10. The court's task is to ascertain the objective meaning of the language which the parties have chosen to express their agreement. It has long been accepted that this is not a literalist exercise focused solely on a parsing of the wording of the particular clause but that the court must consider the contract as a whole and, depending on the nature, formality and quality of drafting of the contract, give more or less weight to elements of the wider context in reaching its view as to that objective meaning. …

119.   However, the Defendants submitted that these embodiments are not relevant to construction and are ignored for the purposes of determining what the claim means. I was not shown any authority in support of this submission. Instead, counsel for the Defendants said that it was based on first principles, by reference to what the reasonable person would do when faced with the Patent. In this regard, she reminded me of the passage of Lord Hoffman in *Kirin-Amgen Inc v Transkaryotic Therapies Inc* [2004] UKHL 46 at [32], where he explained that construction is concerned with "*what a reasonable person to whom the utterance was addressed* [i.e. the skilled person] *would have understood the author to be using the words to mean*". Counsel for the Defendants argued that since the

skilled person was told that certain embodiments fell outside the claim, they would not think they were pertinent to the invention and so would ignore them. Alternatively, she said that if that teaching was required to understand the claims, then this information adds matter over the application and extends protection over the B specification.

120. I reject the Defendants' submission for the following reasons. First, I do not think that the passage to which I was referred in *Kirin-Amgen* is on point. That passage emphasises that construction is determined through the eyes of the skilled person and is based on what he/she would understand the words of the claim to mean. However, it says nothing about the skilled person ignoring parts of the description for that purpose. Secondly, the submission is contrary to principles (ii) to (iv) of *Virgin* as quoted above, which require construction of the claims in the context of the description as a whole (as argued by the Claimant). Thirdly, it is also contrary to common sense. In my judgment, the skilled person will take heed of the parts of the description which are expressed to fall outside the claim just as much as those parts which fall within it. This is because they still serve to help the skilled person understand the scope of the claim and what the words of the claim mean in that context. Fourthly, if the express teaching that an embodiment is outside the claim impacts on what the claim means and that teaching was added by amendment, it may be that matter has been added or protection has been extended, but that is a different point. It does not provide a basis for ignoring that teaching for the purposes of construction.

The Claims in Issue

121. As noted above, there are four claims in issue for validity. Claims 1 and 2 are method claims and claims 7 and 8 are systems claims. However, neither party suggested there was a substantive distinction between the method and system claims, and they focused their submissions on the method claims. Moreover, the only difference between claims 1 and 2 is where the decoding occurs: in claim 1, decoding is undertaken by the portable device, whereas in claim 2 it is undertaken by the server. As a result, it is sufficient to address the arguments by reference to claim 1.

122. Claim 1 provides as follows:

> A method comprising:
> a portable device:
>> obtaining a graphical encoded information item which is displayed on a display of a computing apparatus, wherein the computing apparatus comprises the display and an electronic apparatus, and wherein the display is a sign;
>> decoding the encoded information from the encoded information item;
> and
>> transmitting a first message to first server apparatus, the first message including the decoded information and a first identifier identifying the device or a user of the device, wherein the decoded information includes an apparatus identification information item for allowing identification of the computing apparatus,
>>> the first server apparatus:
>>>> receiving the first message from the device;
>>>> establishing the identity of the user of the device, where establishing the identity of the user comprises using the first identifier to determine if the user is registered with the first server apparatus;

in response to establishing the identity of the user, authorising the user to access a service; and:

using the apparatus identification information item to transmit a signal to the electronic apparatus, and

the electronic apparatus providing the service to the user.

Issues of construction

123.   There were three issues of construction, as follows: (i) meaning of "wherein the display is a sign"; (ii) meaning of "the computing apparatus comprises the display and an electronic apparatus"; and (iii) meaning of "first message". Issues (i) and (ii) come from the third integer of the claim, which states: "*obtaining a graphical encoded information item which is displayed on a display of a computing apparatus, wherein the computing apparatus comprises the display and an electronic apparatus, and wherein the display is a sign*". As a result, it is more convenient to consider issues (i) and (ii) together. This is consistent with the fact that it is important to consider this integer as a whole, a point which the Defendants urged upon me and which I accept.

124.   I also bear in mind the limited role that expert evidence can play in relation to the question of construction. Beyond evidence relating to terms of art, construction is a matter for the court and not the experts: see *Qualcomm v Nokia* [2008] EWHC 329 per Floyd J (as he then was) at [9]-[10].

Meaning of "wherein the computing apparatus comprises the display and an electronic apparatus, and wherein the display is a sign"

125.   Starting with the wording of the integer, the first part of the integer requires that the graphical encoded information item (e.g. a barcode or QR code) is displayed on a display of a computing apparatus. The second part of the integer requires that the computing apparatus comprises the display and an electronic apparatus, and that the display is a sign. Note the use of the definite article twice in the second part of the integer ("*the display*") which clearly refers back to the display of the computing apparatus in the first part of the integer.

126.   It is clear from the language of the integer that the display is a part of the computing apparatus. It may or may not be physically distinct or separate from the electronic apparatus of which the computing apparatus is also comprised, and which must also be present.

127.   I heard evidence about the meaning of a "display of a computing apparatus". Dr Berisso in chief said that the "display" was a technical term that meant "a computer screen or monitor or similar electronic display on any computing apparatus". He also said that "computing apparatus" would be understood to encompass anything containing an electronic memory processor that is able to process messages from network connections, process inputs and control outputs.

128.   Prof Martin did not address this in his written evidence, but in cross-examination he agreed that where the term "display" is used in the context of a computer it meant a screen or monitor or something displaying output. In this context, he was shown various dictionary extracts which defined "display" as follows:

27

i)   Oxford Dictionary of Computing, 2008, which defined "display" as "a device that can be attached to a computer in order to present transient images, textual or pictorial, on its screen";

ii)   Microsoft Computer Dictionary, 5th Edition 2002, which defined "display" as "the visual output device of a computer which is commonly CRT-based video display"; and

iii)   Free Online Dictionary of Computing, last updated 1996, which defines "display" as a "monitor".

He agreed that these definitions were all consistent with the technical meaning of display.

129. However, Prof Martin stressed that the phrase "computing apparatus" (which is used interchangeably at various points in the Patent with "computer apparatus") was not a technical term. The thrust of his evidence was that a display in the context of computing apparatus was not necessarily the same as a display in the context of a computer.

130. Dr Berisso was also cross-examined on this point. He agreed that "computing apparatus" was not a term of art. He confirmed that in the context of the building security embodiment, the skilled person would not expect to see a general-purpose computer but that instead the computing apparatus would be some kind of small, embedded computing device with a processor, attached to the door lock functionality. He said that the phrase "display of a computing apparatus" was "*an overly complicated way of phrasing it, of describing a computer monitor*", but he accepted that the skilled person would not expect to see a traditional computer monitor at the door lock.

131. The Defendants submitted that the upshot of this evidence was that "display" is a term of art and the term did not lose that technical meaning just because the claim referred to it in the context of "computing apparatus" instead of a computer. I do not agree. There was no dispute on the evidence that the term "computing apparatus" was not a term of art. In my judgment the term is broader than a conventional computer (such as desktop or laptop) and is intended to encompass any kind of apparatus that has computing functionality. As a result, the term "display" in the context of "computing apparatus" does not have the same technical meaning as it does in the context of a conventional computer, and the skilled person would not understand its meaning in the context of the claim to be limited to a computer monitor or conventional computer display.

132. Alternatively, the Defendants argued that even if "display of a computing apparatus" as a composite phrase has no technical meaning, it must be referring to some kind of electronic display because it is "a display <u>of</u> a <u>computing</u> apparatus". In this context I think it is more appropriate to consider the wider phrase that the "*graphical encoded information item … is displayed <u>on</u> a display <u>of</u> a <u>computing</u> apparatus*". I agree that the natural reading of this language on its face is that the display is an electronic display, which is capable of displaying the encoded information item.

28

133. However, the Claimant pointed to the next part of the integer, "*where the computing apparatus comprises the display and an electronic apparatus*" and argued that since it is only the apparatus that is stated to be electronic, the skilled person would understand that the display was not. I reject this argument. In my view, the adjective "electronic" is merely used to differentiate that part of the computing apparatus that undertakes the processing functionality from that part of the computing apparatus that displays the output. I do not think that the skilled person would understand it to indicate that the display is not electronic.

134. Even so, that is not the end of the analysis, since I must also consider the claim in the context of the description and the inventor's purpose.

135. In terms of the description, the Claimant relied heavily on the passage from the building security embodiment on p.22 of the Patent which I set out above at paragraph 107 as providing context for its construction that the claim is limited to a display that is a static sign (i.e. a sign which is not electronic and which does not change between transactions). I repeat that passage here for convenience.

> In such an embodiment, the computing apparatus 10 may comprise an electronic door lock. The encoded information item 112, 312, such as a GO as described above, may be displayed on a sign geographically proximate to the electronic door lock. In embodiments outside the scope of the claims, the GO 112, 312 may be provided on an electronic display geographically proximate to the electronic door lock. In such embodiments, the encoded information item may be periodically updated following receipt of signals from the first server apparatus 14.

136. There are several points which come out of this passage which the Claimant relied on and that warrant consideration.

137. The first point from the passage is that the GO is said to be displayed "geographically proximate" to the electronic door. That does not seem to present any conceptual difficulties. It suggests that the GO is physically located close to the electronic door, and there are obvious practical reasons why that would be appropriate in the context of this embodiment. It also suggests that the GO is separate from the electronic door. This is consistent with and provides context for my view that the display and electronic apparatus of the claim do not have to be part of the same device (see paragraph 126 above). The Claimant submitted that, properly construed, the claim required the sign to be geographically proximate to the electronic apparatus, but I do not think that the skilled reader would understand the claim to be limited in this way because geographical proximity between the display and the electronic apparatus is not required for the invention to work (albeit that it may be a convenient or practical implementation for certain applications).

138. The second point from the passage is that the GO "may be displayed <u>on a sign</u>" (emphasis added). By contrast, a GO "provided on an electronic display" is outside the scope of the claim. Based on this teaching, the Claimant argued that the requirement of the claim that "the display is a sign" must be understood in context to exclude an electronic display. I accept that, whatever "sign" means, it does not mean an electronic display, although that is also not the end of the analysis.

139. The third point from the passage is that it teaches that the encoded information item (i.e. the GO) may be updated periodically following receipt of signals from the first server apparatus. The Claimant argued that this teaching only relates to the embodiments outside the scope of the claims. It points to the opening phrase of the last sentence which starts "In <u>such</u> embodiments…" (emphasis added) and says that this phrase only links back to the previous sentence because (i) the use of the plural "embodiments" must relate back to the plural "embodiments" identified in the previous sentence (i.e. those said to be outside the scope of the claims) and (ii) the use of "such" is intended to limit the teaching to that subset of embodiments. The Claimant also said that it makes sense to limit the teaching in this way, since the requirement for periodic updating by way of signals from the first server is only consistent with a GO that is provided on an electronic display. As a result, it submitted that the skilled reader understands that it is only the embodiments where the GO is provided on an electronic display that can be updated from time to time.

140. As to this point, the Defendants argued that the reference to "such embodiments" refers to the whole passage, and hence that it applies both to the embodiments within and outside the scope of the claims. They submitted that this reading is supported by a different passage on p.25 lines 8-9 which states as follows:

> In some embodiments, the encoded information item 112, 312 may be changed periodically, for example, by updating the verification item. In such embodiments, when the verification item is not created by the same entity that is responsible for checking it, the verification item is transmitted to the checking entity each time it is updated.

141. As noted above (paragraph 100), the verification item is optional information within the GO and which allows verification of the GO to ensure that it is not a fraud.

142. The Defendants submitted that the passage on p.25 is not limited to any particular embodiment and that the skilled reader is not told that it only relates to embodiments which fall outside the scope of the claim. As a result, the Defendants said it provides a general teaching that the GO may be changed from time to time and reinforces the view that the last sentence of the passage on p.22 of the Patent would not be understood by the skilled reader to relate only to the electronic display that is outside the scope of the claim.

143. I prefer the Claimant's argument on this point and agree that the requirement for periodic updating in the context of the building security embodiment is limited to the electronic display. In my judgment the phrase "In such embodiments" will be understood by the skilled reader to refer back to the previous sentence, namely to "embodiments outside the scope of the claims". That is the normal way to read it as a matter of English within the context of the passage on p.22 of the Patent. I do not think that the later passage which the Defendants relied upon as set out at paragraph 140 above alters the analysis. This is because that later passage makes clear that periodic updating is only required for some embodiments (albeit it does not say which ones). As a result, the way in which I think the skilled reader would understand the passage on p.22 of the Patent is consistent with its later teaching.

144. More generally, the Defendants relied on the following points in support of their construction that the display within the meaning of the claim must be some kind of electronic or digital signage.

145. First, in relation to the passage on p.22, the Defendants said that since the computing apparatus is identified by the reference numeral 10, the skilled reader will refer back to Figure 1 of the Patent where the computing apparatus 10 is introduced. As noted above, Figure 1 is the only figure that is not said to fall outside the scope of the claims. This figure is said to show "a system in which embodiments of the invention can be implemented". It comprises a standard computing apparatus (10) with a controller (100) that can communicate with a display (104). The Defendants relied on the description at p.10 lines 9-11 which states that "*the controller 100 is operable under the control of the computer-readable code to control the other components such as the display 104*". This is clear teaching that the controller of the computing apparatus controls the display, at least in relation to Figure 1. The Defendants submitted that that teaching is consistent with the display being an electronic display whose output is controlled by the controller with computer readable code and said that is how the skilled reader would understand it, consistently with what is shown in Figure 1. They pointed out that there is no reference in Figure 1 to a static, non-electronic sign and, moreover, such a sign could not be controlled by the controller in accordance with this teaching.

146. However, the Claimant countered that this argument did not take into account that Figure 1 related to a system (i.e. hardware capable of implementing a method) rather than to the method itself. It also pointed to the passage on p.22 from lines 6 to 11 which introduces the embodiments and which I set out at paragraph 104 above. It argued that this passage makes clear that the implementation of the invention in the form of the embodiments may only include some of the features of the system already described. As a result, it said that there was no difficulty with the fact that the system as described in Figure 1 comprised features which are not used in the method as claimed. I think that there is some force in this.

147. Secondly, the Defendants also noted that the reference numerals 112, 312 in the passage on p.22 of the Patent refer to the GO in Figures 2 and 3 respectively. In both these Figures, the GO is shown to be displayed on a computer screen. Whilst their primary position was that the skilled reader would ignore the teaching relating to Figures 2 and 3 since they fall outside the scope of the claims, the Defendants submitted that if they were wrong on that point (which I have held they are), then this teaching simply reinforces the view that the display is electronic.

148. Thirdly, the Defendants reminded me of Dr Berisso's evidence that he understood the phrase "wherein the display is a sign" to refer to some kind of computer display more akin to what would be considered signage. They submitted that this evidence was consistent with the sign being a subset of an electronic or digital display, even if "display" is not a term of art (which I have held that it is not).

149. Fourthly, the Defendants also referred to the teaching on p.26 from line 9 which states as follows:

> The provision of the encoded information item reduces the possibility of a so-called "man-in-the-middle attack". The invention is particularly effective in this respect in embodiments in which the computer program code for generating the encoded information item is stored on the computer apparatus 10 and is configured such that the encoded information item is only provided (i.e. displayed, emitted, output etc.) when direct communication with an application running on the web server 14; 16 is established.

150. The Defendants submitted that this teaching could only apply to a GO displayed on a computer screen but not to a sign which is static in the sense of not being electronic and not changing between transactions. In cross-examination, Prof Martin accepted that the skilled person would understand this teaching to require the display of the GO on a computer screen. It follows that if the Claimant's construction is correct, it means that this advantage of the invention is lost. This was accepted by the Claimant in argument. The Claimant also accepted that the advantage set out at paragraph 113113.ii) above could not be achieved with a static sign. However, it pointed out that the other stated advantages of the invention were still available when the claim was limited to a static sign.

151. This leads on to a consideration of the inventor's purpose. The purpose of the invention is intended to provide secure access to services. I agree with the Claimant that this is primarily achieved by using a separate device such as a mobile to read the GO and communicate with the server, since this takes the authentication process "out-of-band" and separates it from the computer apparatus that provides access to the service. This purpose is achieved with either party's construction even if some of the other advantages cannot be obtained on the Claimant's construction as I have just said. I do not think that this matters, particularly as some of the advantages relate to optional features in any event.

152. Drawing the threads of these competing arguments together, the real difficulty is that different parts of the Patent's teaching appear to be in direct conflict. I accept that the points made by the Defendants as summarised above demonstrate that some of the teaching is clearly directed at (and in some cases limited to) an electronic display. This is also the more natural reading of the claim in isolation as I have said, since a display of a computing apparatus would generally be understood to be an electronic one.

153. However, I cannot ignore the key passage on p.22 of the Patent which is the only passage that sheds any light on what "sign" means and provides important context against which the claim is to be read and understood. This is the only reference to "sign" in the description, and hence the only place where the skilled reader gets any direct teaching as to what it means in the context of the claims (it was common ground that "sign" is not a term of art). As a result, in my judgment it is a passage to which the skilled reader will attach significant weight. The passage says expressly that the GO may be displayed on a sign but that an electronic display is outside the scope of the claim. The only way to make sense of this teaching is that the patentee intended a sign within the meaning of the claim to be something which is not an electronic display. Moreover, since the option for periodic updating in the context of this passage only relates to the electronic display (as I have explained at paragraph 143 above), the skilled reader will understand that the sign is not electronic and does not change between transactions.

154. In the circumstances, after anxious consideration and with some hesitation, I have reached the view that the Claimant's construction of this integer is to be preferred. I have found this the most difficult issue to decide in this case because of the conflicting teaching in the Patent. To resolve construction in favour of either party effectively requires the skilled reader to ignore the teaching that the other party relies on. However, I consider that the Claimant's construction is consistent with *Virgin* principles (v) – (vii). In particular, since the patentee has deliberately limited the claim to a display on a sign, this limitation cannot be disregarded even though it conflicts with some of the teaching of the Patent and does not provide all the advantages of the invention that an electronic display would bring. I do not think that conflicts with the inventor's purpose for the reasons I have given.

155. It is important to note some consequences of the Claimant's construction, since they have a bearing on some of the other issues that I have to decide. First, the Claimant's construction is predicated on the fact that a sign which cannot be updated is not electronic. However, the corollary of that argument is that a sign which can be updated is necessarily electronic. That is something which the Claimant's counsel accepted in oral closings. This concession is important in the context of added matter and extent of protection (see further below). Second, the Claimant's construction is based on a broad interpretation of "computing apparatus" which necessarily includes the situation where the display and electronic apparatus are not in direct communication with each other and where the display has been generated independently of the electronic apparatus. This is important in the context of anticipation and obviousness (see further below).

The First Identifier Issue

156. This issue relates to the following integers of claim 1:

> "transmitting a first message to first server apparatus, the first message including the decoded information and a first identifier identifying the device or a user of the device, wherein the decoded information includes an apparatus identification information item for allowing identification of the computing apparatus"; and

> "the first server apparatus: receiving the first message from the device; establishing the identity of the user of the device, wherein establishing the identity of the user comprises using the first identifier to determine if the user is registered with the first server apparatus"

157. The Defendants submitted that these integers require the first message to comprise a first identifier which identifies the device or the user and enables the first server to determine if the user is registered for the service or not. They said that the word "first" must be given its natural meaning and that, as a result, this must be the first time which the device or user is identified. They also said that the effect of these integers is that only one message and one server are required before the user can access the service. The Defendants argued that if the device has previously been identified by the system, then the system falls outside the scope of the claims.

158. This point of construction matters for infringement because the Shell system utilises two messages which are conveyed to the server which identify the user, and with the later iterations, each of those messages goes to a different server.

159. The Claimant submitted that this construction is wrong, and that the word "first" merely acts as a means of distinguishing that message from other messages in the description. It said that the claim does not preclude a system where there has been an earlier message sent before the "first message" which also serves to identify the user. It pointed to the passage on p.20 lines 20-25 which provides that, prior to preparing and sending the first message, the application on the portable device may request security information to be provided by the user via the user interface of the device so as to allow the identity of the user to be verified. This can be done by a variety of different means, including a pin, a password or biometric information. However, it is important to note that this optional preliminary step relates to identification of the user by the device and not by the server, so I do not think that this passage is directly relevant. What is more useful is the description of Figure 2 which differentiates the "first" message and server from a "second" message and server. I think that the skilled reader would understand these terms to be used in context as a means of differentiation and not as a limit on the number of messages which can be sent. Whilst I appreciate that this Figure is outside the scope of the claims, it enables the skilled reader to understand why the term "first" appears in the claims at all.

160. It follows that the claim is not limited to a situation where the server identifies the user or device once and once only. All that it requires is that the "first message" is transmitted to the server and that it includes the decoded information and the means to identify the device or user. It does not limit how many messages are sent or whether other messages can be sent to the server identifying the user before the "first message". Whilst multiple messages would be less efficient, they do not undermine the purpose of the invention which is to provide secure access to services. In my judgment, the word "first" is used as a means of differentiating the message and the server from other messages and servers, and no more.

ADDED MATTER

Relevant principles

161. The law in respect of added matter is well established and the principles were not in dispute. I was referred to the well-known summary in *Vector v Glatt Air Techniques* [2007] EWCA Civ 805 at [97]-[102]. I particularly bear in mind that subject matter will be added unless it is clearly and unambiguously disclosed in the application as filed, and that it is important to avoid hindsight in the sense that the skilled person reading the application has not seen the amended specification and so does not know what they are looking for.

162. Both parties also referred me to *Nokia OYJ (Nokia Corporation) v IPCom GmbH & Co KG* [2012] EWCA Civ 567 where Kitchin LJ (as he then was) explained the concept of an intermediate generalisation at [56]-[60].

The Issue

163. The Defendants attacked the validity of the Patent pursuant to s.72(1)(d) Patents Act 1977, arguing that subject matter relevant to the invention has been added to the C specification beyond that which was disclosed in the application as filed.

They put the argument in three ways. First, they said that there is no clear and unambiguous teaching in the application as filed that the display can be non-electronic. Second, in the alternative, if there is such disclosure in the application, then it is only in the specific context of the building security embodiment and introducing it into the claim amounts to an impermissible intermediate generalisation. Third, they argued that matter has been added by the addition of references to "electronic apparatus" in the claims which did not appear in the application as filed.

164. These arguments are based on two key changes between the application as filed and the C specification. The first set of changes are amendments to the claims. As with the other parts of the case, I can focus on claim 1. The amendments are indicated in the text below (additions underlined, deletions struck through).

> A method comprising:
> a portable device:
> > obtaining a graphical encoded information item which is displayed on a display of a computing apparatus, <u>wherein the computing apparatus comprises the display and an electronic apparatus, and wherein the display is a sign</u>;
> > decoding the encoded information from the encoded information item;
> and
> > transmitting a first message to first server apparatus, the first message including the decoded information and a first identifier identifying the device or a user of the device, wherein the decoded information includes an apparatus identification information item for allowing identification of the computing apparatus,
> > the first server apparatus:
> > > receiving the first message from the device;
> > > establishing the identity of the user of the device, where establishing the identity of the user comprises using the first identifier to determine if the user is registered with the first server apparatus;
> > > in response to establishing the identity of the user, authorising the user to access a service; and
> > > ~~providing the service to the user via the computing apparatus~~ using the apparatus identification information item <u>to transmit a signal to the electronic apparatus, and</u>
> > > <u>the electronic apparatus providing the service to the user</u>.

165. The second set of changes relate to the teaching that Figures 2 and 3 and the ATM and self-service shopping embodiments are all now outside the scope of the claim, whereas in the application as filed they were said to be illustrative of the invention.

166. It is worth noting the chronology in respect of these amendments. The Patent was granted on 8 May 2013. The first iteration of the Shell system was introduced on 22 July 2015 and the Claimant notified the Defendants of the existence of the Patent sometime in the second half of 2017. Subsequently, the second iteration of the Shell system was introduced in 2017 and the third iteration was introduced in about September 2018. The amendments to the C specification were published on 2 August 2018. The fourth iteration (not said to infringe) was introduced on 19 August 2019. Pursuant to s.27(3) Patents Act 1977 the amendments have the effect and are deemed always to have had effect from the grant of the patent.

<u>Disclosure that the display can be static?</u>

167. The Defendants submitted that there is no clear and unambiguous disclosure in the application as filed that the display can be a static (i.e. unchanging, non-electronic) sign for the following reasons.

168. First, they argued that "display" of a computing apparatus is a technical expression or a term of art. I have already rejected this argument in the context of construction of the Patent, above.

169. Second, they pointed to various aspects of the description in the application as filed which teach the skilled reader that the display is electronic. These include:

    i)   The disclosure in respect of Figure 1, which teaches the skilled reader that the controller of the computing apparatus operates under the control of computer-readable code to control the display. It follows that it is an electronic display. This is also clear from the Figure itself, since the display is in electronic communication with the controller. Dr Berisso gave unchallenged evidence that the skilled reader would understand the display to be a digital display that the computing apparatus is able to control. Whilst this evidence was given in the context of the C Specification, it applies equally to the application as filed.

    ii)   Figures 2 and 3, which both show an electronic display in the form of a laptop computer screen. I also note that the description relating to Figure 2 provides that the GO is displayed "on or by" the computer apparatus (application p.11 lines 1-3). The teaching in respect of Figure 3 is the same (application p.17 line 29-32). In each case, it is clear that the GO is displayed on the computer apparatus (i.e. on the computer output, illustrated as a laptop screen in the Figures) or by the computer apparatus (in the sense the computer apparatus generates the display).

    iii)   The check-out device and ATM alternative embodiments, both of which comprise a display on a screen. In respect of the former embodiment (which is not in the B or C Specifications), the invention may be implemented so that a shopper can pay for goods at a computing apparatus which is a checkout device (10). The description provides that once the goods to be purchased have been scanned through the checkout device, it "produces and displays an encoded information item 112, 312, in this example a GO". Similarly, in respect of the latter, the description states that the ATM "produces and displays an encoded information item 112, 312". Whilst no further details about the display are provided, it was common ground that the ATM will comprise an electronic screen.

    iv)   The teaching on p.26 from line 9 set out above (see paragraph 148) that the invention is particularly effective in avoiding man in the middle attacks when the GO is only displayed when direct communication with the server is established.

170. Third, they argued that the passage relating to the building security embodiment does not provide clear and unambiguous teaching that the display can also be non-

electronic. The text of this passage is different in the application as filed, in that nothing is said to fall outside the scope of the claims. It provides as follows:

> "According to one alternative embodiment, the invention can be implemented in a building security system. In such embodiment, the computing apparatus 10 may comprise an electronic door lock. The encoded information item 112, 312, such as a GO as described above, may be displayed on a sign geographically proximate to the electronic door lock. Alternatively, the GO 112, 312 may be provided on an electronic display geographically proximate to the electronic door lock. In such embodiments, the encoded information item may be periodically updated following receipt of signals from the first server apparatus 14 (or from the second server apparatus 16 if the system is as shown in Figure 2)."

171. In this regard, the Defendants pointed to the fact that the encoded information as illustrated in Figure 2 (112) and Figure 3 (312) are both electronic displays. They submitted, therefore, that the skilled reader will understand "sign" to be digital or electronic. They said that this understanding is reinforced by the subsequent teaching that the encoded information can be updated periodically following receipt of signals from the server because this is only possible with respect to an electronic display. In any event, they argued that there is no clear and unambiguous disclosure in this passage of a sign that is static, either in the sense that it is not electronic or that it cannot be changed.

172. Lastly, the Defendants pointed to the language of the claims of the application, which requires "a graphical encoded information item which is displayed on a display of a computing apparatus". It is trite law that the claims of the application are part of the disclosure (although there can be a difference between what is disclosed by a claim and what falls within its scope). The Defendants argued that this wording teaches that the display is a display of a computing apparatus and will be understood in context of the application as a whole to relate to an electronic display.

173. By contrast, the Claimant argued that the application teaches that the display can be electronic or non-electronic. In this regard, it relied on the passage from the building security embodiment set out above (paragraph 170) and made two main points.

174. First, it said that since one embodiment in the passage relates to an electronic display, the other alternative embodiment that relates to a sign must be something which is not electronic. This is the same submission that I accepted in respect of the construction of the Patent, but it is important to note that the context here is different. In respect of the Patent, the teaching is that only the electronic display can be periodically updated but that it falls outside the scope of the claim. That teaching directly impacts on what the reader understands by the word "sign". By contrast, in the application as filed, the teaching that the electronic display falls outside the scope of the claim is not present. Instead, the skilled reader is taught that the display can be an electronic display or a sign, and both are within the scope of the claims. As a result, whilst the skilled reader would appreciate that the patentee intended for the concept of the sign to be different in some way from that of the electronic display, there is no reason why they would think that the sign will not be electronic. To the contrary, Dr Berisso gave unchallenged evidence that the skilled reader would understand "sign" in this context to relate

to some kind of digital sign including e-paper screens, LCDs or LEDs. This evidence was consistent with the agreed CGK at paragraph 65 above.

175. Second and relatedly, the Claimant submitted that the last sentence about periodic updating only applies to the alternative embodiment where the GO is provided on an electronic display. It said that this alternative embodiment relates to a "class of embodiments" which is why the last sentence is written in the plural. It also said that it makes sense for the last sentence to refer only to the alternative embodiment since only an electronic display can be updated periodically, and that this reinforces the view that "a sign" is not electronic.

176. I reject this submission for the following reasons.

    i)   There was no evidence to support the view that the skilled reader would understand the alternative embodiment to relate to a "class".

    ii)   The submission does not accord with the normal understanding of the text. Since the last sentence refers to "such embodiment_s_" (plural), it must be referring both to the embodiment where the GO is provided on an electronic display and to the embodiment where the GO is displayed on a sign. In my judgment, the skilled reader will understand this passage to teach that where the GO is displayed on a sign or an electronic display it can be updated periodically following receipt of signals from the server. Note that this is another point where I have reached a different decision from the Patent, again because the teaching and context is different. In the Patent, the addition of the phrase "In embodiments outside the scope of the claims" changes the sense of the next sentence and means that it is only understood to apply to the electronic display.

    iii) I agree with the Defendants' argument that it must follow that the sign is digital or electronic, albeit that it is different from an electronic display in some way. Crucially, this must follow even on the Claimant's argument, since (as I noted above in the context of construction) it accepted that only electronic signs can be updated periodically.

    iv)   The submission was circular. The Claimant argued that the last sentence could not apply to the sign because it was not electronic, whilst also suggesting that the sign could not be electronic precisely because the teaching about periodic updating did not apply to that embodiment.

177. In any event, I agree with the Defendants that there is no clear and unambiguous teaching that the sign can be static. Without hindsight, I do not think it would even occur to the skilled reader reading this passage in the context of the application as a whole that the invention could be implemented using a sign that is not electronic or which cannot be changed.

178. As a result, I reject the Claimant's argument that this passage teaches two alternative forms of display; one that is electronic (the display) and one that is not (the sign). Not only is that argument not supported by the text of the passage itself for the reasons I have just given, it is also not supported by the wider

teaching of the application, all of which is consistent with an electronic display or sign.

179. It follows that if the claims of the Patent in the C Specification are limited to a static sign (as I have held), they disclose matter which is central to the invention but was not part of the application as filed. In the circumstances, the claims are bad for added matter and must be revoked.

Intermediate generalisation

180. In light of this finding, formally I do not need to address the alternative argument in respect of intermediate generalisation, since this was only pursued as a fallback and in circumstances where the specification of the application teaches use of a sign or display that is not electronic. However, since I heard argument on it, I should address it briefly.

181. The Defendants argued that if the disclosure of the application as filed teaches use of a display that can be non-electronic, it is only in the context of the building security embodiment and in circumstances where the skilled reader does not understand that it has any inventive significance or any general applicability to the invention. Moreover, they said that some of the features of the embodiment have been "cherry-picked" and put into the claim whilst others have been left out. The Defendants did not say expressly what those features were, but I understood them to relate to the fact that the embodiment is specific to computing apparatus comprising an electronic door lock whereas the claim relates to computing apparatus more generally.

182. By contrast, the Claimant submitted that if the application discloses both electronic and non-electronic displays, narrowing the claim to one which can only be non-electronic display does not add matter. It also submitted that the only generalisation in the claim as amended is that it <u>covers</u> different kinds of computing apparatus related to different services beyond the electronic door example, but that does not affect the way in which the invention works and does not amount to new disclosure. In this regard, it reminded me of what Floyd LJ had said in *AP Racing Ltd v Alcon Components Ltd* at [28]-[40].

183. I prefer the submissions of the Claimant on this issue and agree that if (contrary to what I have held above), the application had disclosed both electronic and non-electronic displays, the amended claims would not amount to an intermediate generalisation.

Electronic Apparatus

184. Finally, I deal with the point about "electronic apparatus". This relates to the additional text that has been added to the claim by amendment which requires that "*the computing apparatus comprises the display and an electronic apparatus*" and "*using the apparatus identification information item to transmit a signal to the electronic apparatus, and the electronic apparatus providing the service to the user*".

185. The Defendants pointed to the text of the application which provides that the encoded information item includes an apparatus identification information item which allows for identification of the computing apparatus. The server performs an action on the decoded information and sends a signal to the computing apparatus based on the apparatus identification information item (see p.2 lines 6-20; p.4 line 26-28; p.5 lines 7-13; p.6 lines 1-7). The Defendants submitted that this teaches that the apparatus identification information item is transmitted to the computing apparatus and not to the electronic apparatus. They also pointed to the text of the application which states that the service is provided by the first server apparatus (p.13 line 22) or by the second server apparatus (p.15 line 33 – p.16 line 1). The Defendants said that this is different from the amended claim, which discloses that the electronic apparatus provides the services to the user, and that the amended claim comprises new disclosure about the invention that cannot be found in the application at all (or certainly not in a way that is clear and unambiguous).

186. By contrast, the Claimant argued that "electronic apparatus" is clearly disclosed within the building security embodiment. So far as I understand the argument, this is because for that embodiment the computing apparatus comprises an electronic door lock, and the Claimant equates this to electronic apparatus. The Claimant also argued that the amendments to the claim come directly from the text in the application, referring to the passage on p.22 line 32 which states "*the first server apparatus 14 transmits a signal to the electronic door lock (using the GO address information item) authorising the electronic door lock to open and thereby to allow the user to pass through the door*".

187. In my judgment, the amendment to the claim which provides that the computing apparatus comprises a display and electronic apparatus does not add matter, since this is consistent with how the skilled reader would understand that term in any event. I do not think that describing the "business" end of the computing apparatus as electronic apparatus changes the disclosure or provides new teaching. However, I consider that the additional final integer, which requires that it is the electronic apparatus which provides the service to the user is new disclosure which changes the way the invention works. I do not agree that the passage the Claimant relies upon as quoted directly above provides support for this amendment. To the contrary, that passage is consistent with the teaching set out in paragraph 185 above to the effect that it is the server that provides the service to the user by authorising the door to open, and not the electronic door itself.

188. Accordingly, this provides a further reason why the claims are invalid for added matter. I should note that this point of added matter arises regardless of the issue of construction of "wherein the display is a sign" and whether the claim is limited to a static sign.

EXTENDED PROTECTION

189. The Defendants also attacked the validity of the Patent pursuant to s.72(1)(e) Patents Act 1977, arguing that the protection conferred by the Patent has been extended by amendments made on 2 August 2019 which should not have been

allowed. Pursuant to s.76(3)(b) of the Act, no amendment of the specification shall be allowed under section 27(1), (general power to amend the specification after grant) if it extends the protection conferred by the patent.

190. Once again, there was no dispute between the parties as to the relevant principles. I was referred to the helpful summary from Birss J (as he then was) in *Hospira v Genentech* [2014] EWHC 3857 at [106]-[108]. Since this issue does not arise very often, I set out the extract in full:

> 106. This rarely comes up at trial in the UK, no doubt because the law is clear and usually easy to apply. The correct approach is to compare the scope of the claims as granted with the scope of the claims as proposed to be amended. In both cases the scope is that of the claims properly construed in accordance with the Protocol. If the proposed amended claim covers something that would not have been covered by the granted claims then the prohibition is engaged.

> 107. Usually to make the argument good the person challenging the amendment needs to identify a concrete thing which did not fall within the scope as granted but which would fall within the scope after amendment if the amendment was allowed. If such a thing cannot be identified in concrete terms, that is usually an indication that there is no extension. Because the prohibition is absolute, the thing need not be commercially realistic.

> 108. The purpose of the prohibition is the protection of the public. Once a patent has been granted, the public can rely on its scope and know that it will not get any wider by amendment. There is no corresponding prohibition pre-grant. The law of added matter is different. It applies both pre- and post-grant.

191. The exercise involves a comparison of the claims in the B Specification (the Patent as granted) with the C Specification (the Patent as amended post grant). In fact, the amendments are the same as those set out above in paragraph 164 because the claims did not change between the application as filed and the B specification.

192. In light of what I have said above in respect of added matter, I can deal with this point quite shortly.

193. Just as with the A Specification, in the B Specification all the Figures and embodiments are included within the scope of the invention as claimed. As I have already explained above, Figures 2 and 3 indicate that the GO is on a computer screen; likewise with the ATM embodiment, it is clear that the GO is displayed on an electronic display.

194. However, the Claimant argued that the claims of the B Specification, properly construed, cover both an electronic display and a static sign.

195. In support of this argument, it relied on the now familiar passage concerning the building security embodiment, albeit that the text is a little different in the B

Specification from the C Specification (but the same as the application). I set out the passage at paragraph 170 above.

196. Consistent with its case in respect of the application as filed, the Claimant submitted that this passage teaches two alternatives: a static sign and an electronic display. However, unlike the C Specification, in the B Specification the embodiment where the GO is provided on an electronic display is not outside the scope of the claims. In my judgment, this has several consequences. First, in the context of this passage, there cannot be any doubt that the last sentence refers to both embodiments of the building security system that are described in the preceding two sentences (i.e. where the GO is displayed on a sign or on an electronic display). Second, this means that the embodiment where the GO is displayed on a sign is one where the GO can be updated periodically following receipt of signals from the first server. Third, it must follow that the sign is digital or electronic, albeit that it is different from an electronic display. Just as with the application as filed, I do not think it would even occur to the skilled reader reading the B Specification that the invention could be implemented using a static sign.

197. As a result, I reject the Claimant's argument that this passage teaches two alternative forms of display; one that is electronic (the display) and one that is not (the sign).

198. The Claimant also relied on the teaching on p.2 lines 15-17 which states:

> "Preferably, the decoded information includes an apparatus identification information item for allowing identification of computing apparatus on, by, or near to which the encoded information object is provided."

199. I do not think that this passage supports the Claimant's argument either. It does not shed any light on whether the display can be electronic or non-electronic or both. It certainly does not follow that merely because the encoded information object may be provided near to the computing apparatus, it cannot be electronic.

200. In any event, even if the Claimant were right and the skilled reader understood either of these passages to teach the use of a non-electronic display, it does not help with the construction of the claim. This is because the claim requires "*obtaining a graphical encoded information item which is displayed <u>on a display of a computing apparatus</u>*" and so is clearly limited to encoded information displayed on the display. Moreover, in my judgment, the skilled reader would construe this claim in the context of the B Specification as a whole to be limited to an electronic display. That is the natural reading of the integer and is consistent with the teaching of the document (contrary to the Claimant's submissions). The claim does not cover a display or sign that is not electronic. If the skilled reader thought that the building security embodiment where the GO is displayed on a sign related to something that was not electronic (which I do not believe that they would), they would simply conclude that the patentee had excluded that option from the scope of the claims.

201. It follows that a non-electronic sign or display did not fall within the scope of claim 1 as granted, but now falls within the scope of the claim as amended post grant. As a result, the protection of the Patent has been extended by an amendment

which should not have been allowed and is invalid for this reason. This reasoning applies equally to claims 2, 7 and 8, which are also invalid accordingly.

SCHMIDT

Disclosure

202. Schmidt is a European patent application (EP 2073160A1) with the title "Communication of coded data from a terminal to a central server via a mobile terminal device by means of a multidimensional barcode". It was published on 24 June 2009, 15 months before the filing date of the Patent.

203. Schmidt concerns a secure method for cashless payment for goods or services. This is summarised by the abstract as follows:

> A terminal of a service provider creates data containing information regarding payment for a service. In this case, said information can contain price information, a preprogrammed destination address for settlement, a unique identification number of the terminal and a destination address for payment confirmation by the service provider. The data produced are encrypted and subsequently coded into a multidimensional barcode. This barcode is retrieved from the terminal before [*sic*] a mobile terminal device of the service user and communicated by means of mobile radio or internet to a central server. The central server performs the payment and confirms to the terminal or to a further mobile that the payment has been carried out.

204. The objectives of the invention are to increase acceptance of cashless payments, and to reduce installation and running costs. These objectives are said to be achieved by providing a secure method for payment transactions and using existing widespread technology (including existing customer equipment in the form of their mobile phones) (p.3 lines 18-26).

205. According to the early parts of the description, payment data is generated by a terminal of a service provider and is encoded in the form of a multi-dimensional barcode. The barcode is "retrieved" from the terminal by the mobile device. The mobile device then transmits "data packets" containing the information coded by the barcode to the server (although there is more teaching about this in the context of Figures 2 and 3 - see below). The terminal is outside the transmission path between the mobile and the server (p.4 line 2 – p.5 line 12).

206. Figure 2 is said to show a transmission system for coded data from a terminal to a server by means of a mobile device in accordance with one embodiment of the invention and enables cashless payment for goods or services. I reproduce the Figure below. It shows the terminal (210), the mobile device (220) and the server (230). According to the description, the terminal can be, for example a taximeter, a ticket-machine for parking, a checkout in a supermarket, part of a fuel-dispensing pump at a filling station or an arbitrary device for determining fees for a service or the value of goods (p.8 lines 19-23). The mobile device can be, for example, a mobile phone, a PDA or a mobile computer (p.8 lines 23-25).

FIG. 2
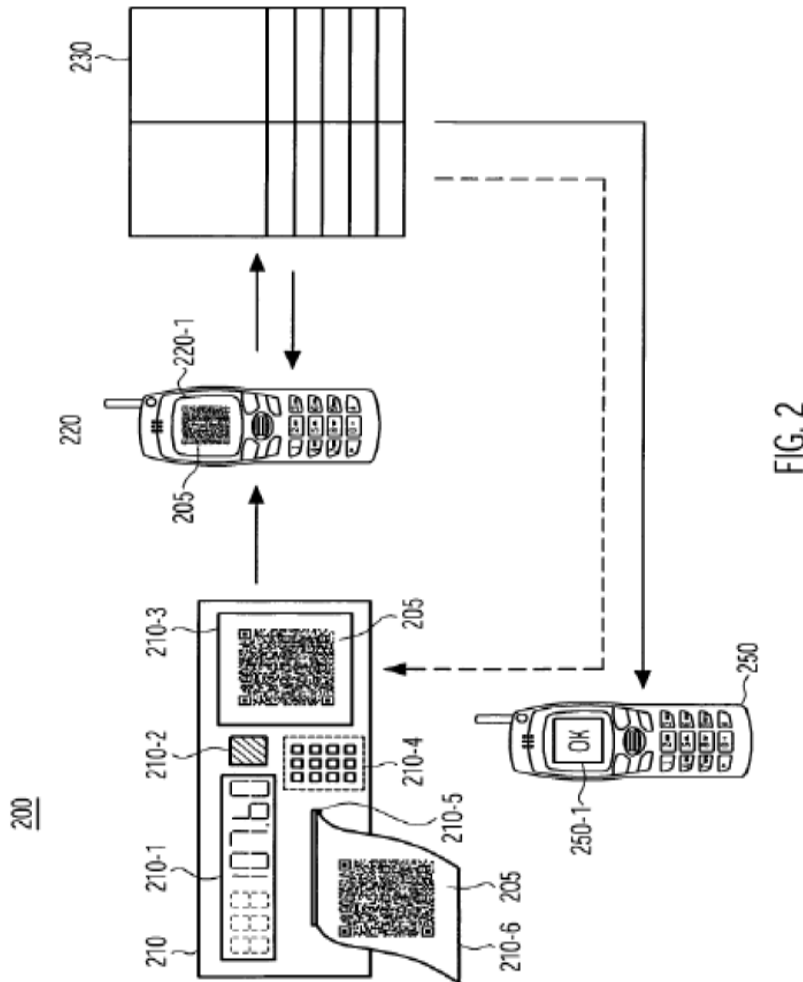
207. In the Figure the barcode is displayed on the terminal display (210-3) and is printed out by the printer unit (210-5). In other words, the encoded information is provided by means of both an electronic display and a non-electronic one. However, the description makes clear that in embodiments of the invention the barcode can be represented on a display or a sheet of paper or both (p.11 lines 15-24).

208. The barcode contains information regarding payment, such as the name and/or account data of the service provider or vendor, the amount to be paid, identification number of the terminal or of the service to be paid, the address of the server, the mobile and/or the terminal, the date/time of transaction, etc (p.11 lines 2-13).

209. The display (210-1) shows as an example, a count determined by the terminal. Depending on the use case, this may represent, for example, the price of the taxi journey so far, the number of minutes intended to be spent parking or in the solarium, the amount of fuel dispensed, etc.

210. Schmidt teaches that for some embodiments the mobile device will have an application which can "interpret the multidimensional barcode and convert it into data packets" (p.12 lines 12-14). I understand this to mean that the mobile device

decodes the barcode information and was the basis upon which the parties agreed that decoding can take place by the mobile. The data packets are transmitted to the server via the mobile network or the internet.

211. However, Schmidt also teaches that in other embodiments the barcode is transmitted to the server as a message with an image of the barcode (in which case the destination address of the server is not part of the coded information in the barcode and is provided by other means) (p.12 line 18 – p.13 line 10). In that case the server decodes the barcode of the message (p.13 lines 24-25).

212. The server can check whether the user has an account or alternatively can allow the user to set up an account or undertake a single transaction. The server also effects payment. In some cases, it can transmit checking information back to the user before payment is made and/or send payment confirmation to the terminal, the mobile device or to a further mobile device (p.13 line 12 – p.15 line 14).

213. Figure 3 shows a method for communicating coded data from a terminal to a server by means of a mobile device in the form of the following flow chart:
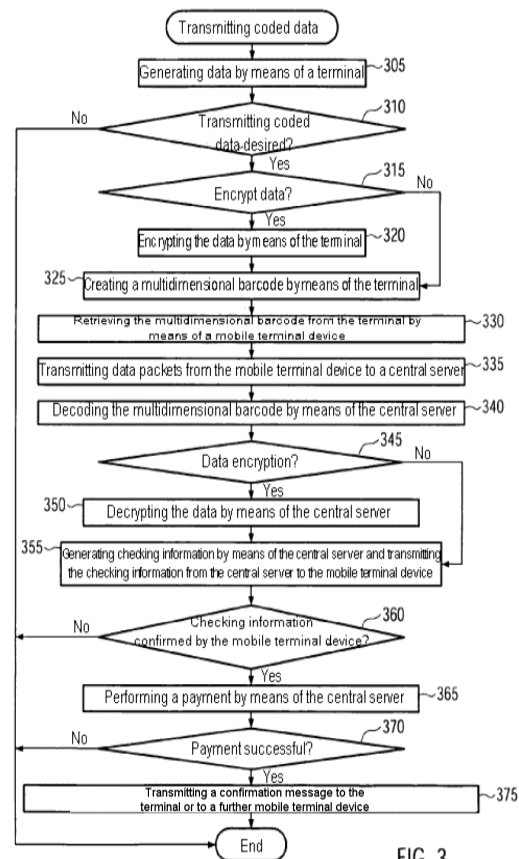

FIG. 3

214. There is a lot of the detail in the description about this Figure, but most of it is not relevant for the purposes of this case. The points that matter are:

i)   In step 305, the terminal generates the data. In some embodiments this can be by way of a count as described in relation to Figure 2. However, in other

45

embodiments the count will be proportional to the amount to be paid or will directly indicate the amount to be paid (p.16 lines 8-17).

ii)   The barcode can be provided to the mobile in a number of ways, including on the display of the terminal or provided by means of a printout on a sheet of paper (p.20 lines 7 – p.22 line 6).

iii)   In some embodiments the mobile device has an application that can decode the barcode and the decoded information is communicated to the server in the form of data packets (p.22 line 22 – p.23 line 2). This is step 335 in Figure 3.

iv)   In other embodiments the barcode is forwarded directly to the server and decoded by it (p.23 line 2 – p.24 line 7). This is step 340 in Figure 3. In this context, the information transmitted at step 335 is an image of the barcode rather than decoded data packets.

215.   Some embodiments or so-called "practical scenarios" are described in more detail from p.27. Of these, the Local Public Transport (LPT) and solarium embodiments were the focus of cross-examination and so I shall only summarise the teaching about them.

216.   The local public transport embodiment is in two parts. The first part relates to a transport stop where there are multidimensional barcodes "depending on the line of the local public transport". I understand this to mean that there is a different barcode for each travel line. The barcodes comprise information including the date of validity of the multidimensional barcodes, stop identification and the line number (p.30 lines 7-9). The passenger uses their mobile phone to read the barcode for the line they have selected. The user may have a specific LPT phone app for this purpose.

217.   The second part of the LPT embodiment relates to a ticket machine with a display. The passenger selects a route, and the machine displays a multidimensional barcode appropriate for that route. The passenger can use their mobile to photograph or scan the barcode from the display or from a paper print out if the machine has a printer unit. The data from the barcode is communicated in an encrypted manner to a server and decoded there. Checking information can be sent back to the passenger who confirms the selection, and payment is then made. Once payment goes through, a ticket may be printed by the machine or sent to the passenger electronically.

218.   With the solarium embodiment, the user selects a time for which they wish to use the solarium. The terminal connected to the solarium thereupon creates a multidimensional barcode which is provided to the user (although the description does not state whether this is by means of a display or a printout). The user photographs the barcode with their mobile phone and transmits the data to a central server. If payment is made, this is communicated by the server to the terminal. The terminal then activates the solarium for the paid time.

Anticipation – relevant principles

219. The applicable legal principles were not in dispute: in order for a piece of prior art to anticipate a patent, it must clearly and unambiguously disclose all the features of the claims in issue (*General Tire & Rubber Co v Firestone Tyre & Rubber Co Ltd* [1972] RPC 457 at 485). Disclosure can be implicit as well as explicit (*Edwards v Boston Scientific* [2017] EWHC 405 (Pat) at [139]).

Anticipation – arguments and analysis

220. It was common ground that Schmidt discloses all the integers of claim 1 (and 7) except the integer "wherein the display is a sign". The arguments in relation to the disclosure of this integer was intertwined with its construction. The Claimant accepted that on the Defendants' construction, claims 1 and 7 of the Patent are anticipated by Schmidt. However, the Claimant maintained that this integer was not disclosed on its construction because the barcode that is generated and used in Schmidt is dynamic in the sense that it changes with every transaction.

221. This was described by Prof Martin in his first report (§45(b)) as follows[1]:

> **Static v Dynamic**. In Schmidt the encoded information contains data relating to a specific payment, which means that it must be dynamic, changing for each individual transaction. This requires the encoded information to be displayed on a screen capable of dynamic representation. In the Patent, according to the claim, this encoded information is displayed in a static form by being physically attached to an apparatus by means of a sign.

222. He went on to say at §46 that Schmidt "does not (indeed could not) consider the encoded information being displayed on a static sign".

223. In reply, he qualified this evidence at §12, where he said:

> In paragraph 7.90 of his Report, Dr Berisso argues that Schmidt teaches us that a barcode can be displayed on a "static, non-digital display such as a printed sign". I acknowledge that Schmidt teaches us that a barcode can appear on a printed piece of paper. However, in Schmidt this piece of paper is a printed version of a specific transaction (in particular, it features the amount charged for a specific taxi ride). This means that the non-digital "display" (the piece of paper) changes every time that the Schmidt system is used. Therefore, I do not agree that in Schmidt the barcode is displayed on a "static sign", which to me is a display that is static across multiple transactions and not changing every time the system is used.

224. I do not accept that Schmidt teaches that the barcode must be dynamic in the sense that it must change for each individual transaction or every time the system is used. There is no express teaching in Schmidt to the effect that the barcode must be different with every transaction. Whether or not that is the case will depend on the nature of the service in question. So, for example, whilst a taxi meter will generate a different barcode for each journey dependent upon the distance that has been travelled, that is not necessarily the case for the LPT embodiment where, for example, the same barcode *could* be used by different passengers for the same

---

[11] Note that the Professor edited this evidence during the course of cross-examination in relation to infringement to delete the phrase "physically attached to an apparatus by means of a sign". This is because the Shell system uses a QR code that is not attached to the petrol pump. See further below.

journey on a particular line. Moreover, there is nothing about the purpose of the invention disclosed in Schmidt which requires the transaction to change every time the system is used.

225. However, I accept that there is no clear and unambiguous disclosure that the barcode *will* be the same with different transactions or will not change between transactions. In this regard, I bear in mind that a disclosure that is capable of being carried out in a way which would infringe a patentee's claim but equally could be carried out in a way that is not infringing will not anticipate a claim (although may still make it invalid for obviousness), and that what is required for anticipation is clear and unmistakeable directions to do what is claimed (see *General Tire* above).

226. The only passage which the Defendants could point to in support of their case was the passage in respect of the second part of the LPT embodiment where it states that "*a ticket machine for traveling is installed at the stop of the LPT, said ticket machine having a display on which, depending on the selection of the route, a multidimensional barcode appropriate to the selected route is then displayed*" (p.30 lines 16-20). They submitted that these words indicate that the barcode is the same for the same routes, but I do not agree. There is no clear and unambiguous teaching in this passage that the barcode will necessarily be the same.

227. The Defendants also said that their reading of this passage was supported by Dr Berisso's evidence in chief, but I do not think he went that far. All Dr Berisso said was that the barcode changes depending on the route that is selected. He did not say anything about whether it remains the same for a particular route.

228. The Defendants submitted that their case was also supported by the cross-examination of Prof Martin, but again I do not agree. Prof Martin was reluctant to accept in the context of the LPT embodiment that the barcode would be the same for different passengers selecting the same route, because he said that the scenario was poorly explained and lots of things about it were not clear. He said it was not clear if the barcode stayed the same or not.

229. It follows that claims 1 and 7 are not anticipated by Schmidt on the Claimant's construction.

230. The Defendants' case was that Schmidt also anticipates claims 2 and 8. This attack necessarily fails for the same reasons as the attack in respect of claims 1 and 7. However, there was an additional point in respect of these claims which I should address for completeness and in case this matter goes on appeal.

231. The additional point was that the Claimant argued that Schmidt only considers the option of decoding information at the mobile device, whereas claims 2 and 8 require decoding by the server. The Claimant maintained that there were no clear and unmistakable directions to use a method or make a system in which decoding of the encoded information takes place by the server. In this context, it submitted that it was not enough to point to the possibility of decoding at the server in isolation; there must be clear and unmistakeable directions to all the features of the claim in combination.

232. The Claimant's case was based on the evidence of Prof Martin in chief. He said at §45(d) of his first report that in Schmidt "the mobile device decodes the extracted information" and at §46 that "Schmidt does not consider the option of server-side decoding". However, Dr Berisso explained in chief (§§7.55, 7.66 – 7.67, 7.108) that decoding can be undertaken by the mobile device or the server. Dr Berisso's evidence was not addressed by Prof Martin in reply and was not challenged in cross-examination.

233. It is not clear to me how Prof Martin was able to form the view that Schmidt does not consider the option of server-side decoding. In my judgment, there is clear teaching in Schmidt that the barcode can be decoded by the server, and it is also clear that this disclosure is in combination with the other features of the claims. I refer to paragraph 210 and paragraphs 213-214 above. Even if one allows for the fact that Prof Martin erroneously limited his understanding on the teaching of Schmidt to the claims (as he explained in cross-examination), his view does not make sense. This is because claim 13, which is dependent on the preceding claims, provides that the server decodes and decrypts the received data packets.

234. It follows that if I am wrong in respect of claims 1 and 7, and those claims are anticipated by Schmidt on the Claimant's construction, claims 2 and 8 are also anticipated. Moreover, since the Claimant accepts that claims 1 and 7 are anticipated by Schmidt on the Defendants' construction, based on what I have said above, it follows that claims 2 and 8 are anticipated by Schmidt on the Defendants' construction.

Obviousness – relevant principles

235. The relevant principles are well known and were not in dispute. I was referred to the familiar extract from *Actavis v ICOS* [2019] UKSC 15 from [60].

236. In addition, I was reminded of the following points:

    i) If a route is obvious to try, that is not undermined by the fact that there may be one or more other obvious routes as well (*Brugger v Medicaid Ltd (No 2)* [1996 RPC] 635, 661).

    ii) However, motive in taking any particular step is a key consideration (*Actavis* at [70]).

    iii) Hindsight must be avoided (*Technograph Printed Circuits Ltd v Mills & Rockley (Electronics) Ltd* [1972] RPC 346 at 362).

    iv) The simplicity of an invention is not an objection to it being inventive (*Haberman v Jackel International Ltd* [1999] RSR 683 at [29]).

    v) The reasons given by the experts for their views are paramount (*Schlumberger v EMGS* [2010] EWCA Civ 819 at [86], *SmithKline Beecham plc v Apotex Europe* [2005] FSR 23 at [52]-[53].

237. I have all these principles well in mind.

Obviousness – arguments and analysis

238. The obviousness case over claims 1 and 7 on the Claimant's construction was based on the LPT and solarium embodiments of Schmidt, and as I have noted above, the cross-examination of both experts was centred on these embodiments.

239. As regards the LPT embodiment, the Defendants argued that it would be obvious to the skilled reader to implement the ticket machine scenario using a barcode which did not change between transactions, for example in respect of different passengers using the same route or in respect of the same type of passenger (e.g. adults) travelling within a particular zone. This was put to Prof Martin in cross-examination and he agreed that this was one possible option for implementation, although he pointed out that there were other ways in which it could also be done.

240. The Claimant criticised this cross-examination. It said that it was based on "the ingenuity of counsel" rather than evidence, and that it was unclear what was being put to the Professor. However, whilst arguably some of the questions could have been better phrased, I watched this cross-examination carefully and believe that Prof Martin understood what was being put to him. This is illustrated by the following exchange at T2/239/5-24:

> Q. And if the skilled person was implementing this, then one way
> 6 of doing the bar code on the printout is to have a bar code
> 7 which represents a selected route?
> 8 A. Well, this is possible, but there are many -- one would
> 9 imagine in any sensible public transport network there are
> 10 many possible routes, so I think the skilled person
> 11 interpreting this would certainly be imagining that there is
> 12 some electronic selection and an electronic way of identifying
> 13 different routes. But, having then selected a specific route,
> 14 it is possible that the bar code displayed is the same for the
> 15 next passenger that walks up and wants that same specific
> 16 route.
> 17 Q. Exactly. It is not just possible, that is a sensible and
> 18 obvious way of implementing this if you are implementing it.
> 19 A. It could be. Again, it depends how their transport system
> 20 works and whether the nature of the traveller also affects the
> 21 ticket that is being sold, so there could be, it seems, likely
> 23   there might be other inputs but in a very simple setting,
> 23 I suppose that could be possible if all passengers were the
> 24   same.

241. The answers that Prof Martin gave are consistent with the observations I made above at paragraph 224 above. In my judgment, it would have been obvious to the skilled reader at the priority date to implement the LPT ticket machine embodiment using barcodes that were the same for different passengers (and hence different transactions) in respect of travel on the same route or line. In this regard, I accept the unchallenged evidence of Dr Berisso that this would be a simple design choice. It follows that it would have been obvious to implement that embodiment using a barcode that is static in the sense that it does not change between transactions. Since this was the only integer in dispute, it follows that claims 1 and 7 are obvious over Schmidt on the Claimant's construction.

242. As to claims 2 and 8, and in case I am wrong about anticipation of these claims, I note that Prof Martin accepted in his written evidence and confirmed in cross-examination that it would be obvious to implement the teaching of Schmidt with server-side decoding. This is consistent with what was accepted to be CGK at

paragraph 89.i) above. It follows that these claims are also obvious over Schmidt on either construction.

243. In light of these findings, I do not need to address the evidence in respect of the solarium embodiment in much detail but do so for completeness and in case of any appeal.

244. The Defendants' case in respect of this embodiment was that it would be obvious to implement it using the same barcode for different users that wanted a tanning session of the same duration. Prof Martin accepted in cross-examination that this was an obvious way to put this part of Schmidt's teaching into effect (i.e. such that the sign does not change between transactions). I think he was right to do so, for the reasons I have set out in paragraph 224 above.

245. However, to get home on obviousness over claims 1 and 7 on the Claimant's construction, the Defendants must also establish that it would be obvious to the skilled reader to implement the solarium embodiment using a sign that is not electronic. Dr Berisso did not address this in chief specifically in the context of the solarium embodiment. He only gave general evidence that a printed sign may work better in certain circumstances, such as when the encoded information contains a URL to direct the user to a website or server or to identify an apparatus, but I do not think that went far enough to establish the Defendants' case.

246. It was suggested to Prof Martin in cross-examination that the solarium may comprise a piece of "legacy" equipment which did not have a terminal and in that situation, it would be obvious to implement the teaching of Schmidt using a barcode printed on a piece of paper instead. The Professor found this line of cross-examination confusing, and I have some sympathies with his position. It was not clear to me why the skilled reader would consider implementing this embodiment without a terminal, particularly when the terminal activates the solarium once payment is confirmed. Moreover, I cannot see that it helps the Defendants since the terminal comprises the computing apparatus of claim 1 of the Patent. It means (as the Claimant pointed out) that the Defendants' attempt to demonstrate that it is obvious to implement the solarium embodiment using a paper sign is predicated on the basis that another integer of the claim is missing. It follows that I do not accept that there was anything in the criticism that the Defendants levelled against Prof Martin to the effect that he had refused to put himself in the place of the skilled person implementing the prior art.

247. It was also put to Prof Martin in cross-examination that it would be obvious to implement the solarium embodiment using a paper sign if the display of the terminal was "not good enough" to display the barcode. Prof Martin accepted that this would be obvious if those constraints existed, but there was no evidence to suggest that they would. I found this line of cross-examination to be contrived and agree with the Claimant's submission that it was based on hindsight.

248. In the circumstances, I would not have held that the Patent is obvious over the solarium embodiment if it had been necessary to reach a decision on this issue.

KILICCOTE

Disclosure

249. Kiliccote is a US Patent (No 7,379,921B1) with the title "Method and apparatus for providing authentication". It is dated 27 May 2008. As the title suggests, it concerns a method and system for authentication. This is summarised in the abstract as follows:

> A system for providing authentication is disclosed. The system includes a server configured to present an image to the user via a computer, the image having information embedded therein, and a portable device configured to: allow the user to capture the image, store predetermined information, capture input information from the user, the input information to be used to ensure that the user is authorized to use the portable device, and generate an output based on the information embedded in the image and the predetermined information. The server is further configured to receive output from the portable device and authenticate the user based on the output. Once the user is authenticated, the user is allowed to access a website via the computer to conduct a transaction with respect to an account associated with the user.

250. The first section is "Background". It starts by identifying the field, stating that the invention relates to secure transactions, and more specifically to methods and devices for providing secure identification, verification and authorisation using a portable secure device.

251. It goes on to provide further background. It notes that authentication can be useful, for example, in relation to e-commerce transactions and that there are many authentication systems known in the art with related methodologies that use a wide range of techniques. Several prior art systems are then described, the details of which generally do not matter for the purposes of this case. However, the authors note the authentication used in respect of credit cards (PIN, numbers printed on the back of the card, etc) may be of nominal effectiveness because they are static (col 1 lines 30-37). The authors state that it is desirable to provide methods and devices that are capable of providing secure transactions in a more efficient manner.

252. The second section, "Summary", sets out a summary of the invention. This starts with a description of the system of the invention, which is the same as the abstract, set out above. There follows a description of the method, which is in equivalent terms.

253. The next sections are "Brief Description of the Drawings" and "Detailed Description". In the opening paragraphs, the Detailed Description states:

> The present invention may be used for a number of different purposes including, for example, authentication, authorization, secure document distribution and guarding against phishing attacks, as will be further described below. The present invention may be used in both the offline and online environments and provide on-demand input capability.

254. It goes on to describe several different embodiments by reference to the figures to which they relate. As with Schmidt, I shall focus on the teaching and embodiments which were the subject of cross-examination. I have not reproduced the relevant figures in the body of this judgment as they are of poor quality and

limited assistance, but they are included in an Annex at the end of this judgment for the benefit of the reader.

255. Figure 1 illustrates a secure device which may be part of a mobile phone, PDA, etc. It comprises a processor, a memory, an image capture device (e.g. a camera), and input and output means. Kiliccote states that the device operates in the manner set out in Figure 2. First, it is used to capture encoded information in an image, for example in the form of a barcode. The information is relevant to the transaction to be conducted. The device also prompts the user to provide identification information via the input (for example in the form of a PIN). The processor of the device then decodes the image and extracts the information. This may include predetermined information stored in the memory of the device, such as address information, personal profile information and payment information. The device also checks the identification information provided by the user to authenticate their identity against information previously provided by the user during registration. Upon successful verification of the user's identity and decoding of the information, instructions may be provided for further action by the user, for use in connection with various purposes described in the various embodiments.

256. One embodiment (described by reference to Figure 3) comprises an authentication process for access to a website. The user visits the website via a computing device and is presented with a log-on screen. After preliminary information is provided by the user (e.g. password), they are presented with an image such as a barcode. This is generated by the website and displayed on the computer screen. It contains embedded information that is used to obtain an authentication code required to access the website. The barcode is scanned or photographed by the user's mobile phone or other secure device, which then derives the relevant information from the barcode. This will include the authentication code, which is displayed on the output screen of the phone. The user can then key in the authentication code into the computer to obtain access to the website. Alternatively, the authentication code can be transmitted to the computer in the form of a radio or sonic signal (if the computer has the appropriate receiver).

257. Kiliccote goes on to explain that this method can also be used to authenticate users for physical access to structures and through entry points such as doors or gates. In addition to the authentication code information, the barcode or other encoded image captured by the secure device may include additional information such as information relating to the website, structure, etc to which the user is gaining access.

258. In another embodiment (described by reference to Figure 9), the secure device can be used to capture an image which is displayed on printed materials "such as books, signs, and catalogs" (col 11 line 61) or on a television or computer screen (col 11 line 61-62) or both (col 11 line 64-66). The image may include embedded information relating to the product or service of interest, information related to the merchant and the internet address of the merchant.

259. There are two different variants described by reference to the Figure 9 embodiment, one where the mobile device interacts with the merchant server and

one where it interacts with a third-party server. The focus of evidence and argument was on the third-party server variant. In this example, the user uses the secure device (e.g. their mobile phone) to scan and decode the image, sending the relevant information to the third party server. The third-party service provider then cooperates with the merchant server to complete the transaction including, for example, transferring the information required to complete the transaction, such as payment and shipping information to the merchant server.

260. There was also some cross-examination on the embodiments described by reference to Figures 10 and 11, but the Defendants disavowed any reliance on those embodiments as part of their closing arguments and so I do not need to address them.

Anticipation – relevant principles

261. I have set out the relevant principles in the context of Schmidt, above.

Anticipation – argument and analysis

262. The Defendants' case of anticipation by Kiliccote only relates to claims 1 and 7, but on both constructions. It was accepted by Prof Martin that most of the integers of claim 1 were disclosed by Kiliccote. The ones in dispute were:

   i)   "which is displayed on a display of a computing apparatus … wherein the display is a sign". There are two points in relation to this integer. One depends on what it means to say that "the display is a sign" – i.e. the key construction point I have addressed above. The other relates to whether there is disclosure in Kiliccote of computing apparatus which is separate to the first server of the claim.

   ii)   "transmitting a first message to a first server apparatus, the first message including the decoded information and a first identifier identifying the device or a user of the device". The Defendants argued that there was implicit disclosure of the first identifier, but the Claimant said that that there are no clear and unmistakeable directions to this integer in combination with the other integers of the claim.

   iii)   "wherein the decoded information includes an apparatus identification information item for allowing identification of the computing apparatus". There is a dispute about whether the apparatus identification information item is disclosed.

263. Starting with the Claimant's construction, which is the one which I have largely accepted, the Defendants framed their case by reference to the Figure 9 embodiment as it relates to printed matter and the third-party service provider.

264. First, the Defendants argued that the barcode in this embodiment is obviously static in the sense that it is not electronic and does not change between transactions. This was accepted by Prof Martin in cross-examination. I agree.

265. Second, the Defendants pointed to the fact that the embodiment comprised two servers, one associated with the merchant (col 12 lines 41-44) and one associated with the third-party service provider (col 12 lines 45-51). They submitted that the "computing apparatus" of claim 1 was comprised of the merchant server and the catalog (or other sign). They pointed out that this was consistent with the Claimant's construction, which necessarily requires that "computing apparatus" is a wide term that covers the situation where the display and the electronic apparatus are not in direct communication with each other, albeit that they are associated in the broadest sense. I agree with this submission, which is consistent with what I have said above in the context of construction and also how the Claimant argued its case on infringement (see below). Prof Martin also accepted in cross-examination that there was teaching in the general summary of Kiliccote (before the embodiments) to the effect that the computing apparatus and the server are separate items.

266. In the circumstances, I reject the Claimant's argument to the contrary that the merchant's server cannot be the computing apparatus of the claim. I found this part of the Claimant's submissions confusing and difficult to follow, but so far as I understood them, the argument was that there had to be some kind of "return path" between the merchant server and the mobile phone and that was not disclosed in Kilicotte. This was not a point that was canvassed in evidence, and in any event does not seem to be relevant to the requirements of this integer or the claim.

267. There was also a suggestion by the Claimant that the catalog of the Figure 9 embodiment could not be the display of the computing apparatus because it is physically remote from the server and there is no relationship or association between them. However, I have rejected the argument that the claim requires the sign to be geographically proximate to the electronic apparatus. Moreover, the claim does not require the encoded item to be generated by the electronic apparatus or for there to be any communication between them. In any event, this point was also inconsistent with the Claimant's case on infringement.

268. Taking these points together, it follows that the integer "which is displayed on a display of a computing apparatus … wherein the display is a sign" integer is disclosed by Kiliccote on the Claimant's construction.

269. Third, the Defendants pointed to col 12 lines 52 – 55 which makes clear that the secure device (e.g. the mobile phone) decodes the information in the barcode and then sends a confirmation to the third party service provider. They argued that this amounted to disclosure of the integers of claim 1 which require decoding of the encoded information by the mobile phone and transmitting the decoded information as a first message to a first server apparatus, both of which I accept. The third-party service provider is the first server apparatus for this purpose.

270. However, the Defendants also argued that as part of this teaching there was an implicit disclosure that "the first message including … a first identifier identifying the device or a user of the device". This was because they said it would not be possible for a user to pay for something unless the user had been identified first. I do not accept this submission. There was no evidence from the experts in their written evidence in support of a case of implicit disclosure and it was not

put to Prof Martin in cross-examination that the skilled reader would understand Kiliccote in this way based on their CGK. In my view, this does not amount to clear and unmistakable directions to do something which falls within this part of the claim.

271. Fourth, the Defendants relied on the teaching in Kiliccote that the barcode of Figure 9 includes the merchant's internet address (col 11 line 66 – col 12 line 6). They submitted that this comprised the apparatus identification information item for allowing identification of the computing apparatus within the meaning of the claim. I accept this submission, which was also consistent with what Prof Martin accepted in cross-examination.

272. Fifth, the Defendants also relied on the teaching that the third-party service provider cooperates with the merchant server to complete the transaction, including e.g. transferring the information required to complete the transaction such as payment and shipping information to the merchant's server (col 12 lines 55-63). They submitted that this satisfied the related integer in claim 1 of "using the apparatus identification information item to transmit a signal to the electronic apparatus and the electronic apparatus providing the service to the user". I accept this submission and agree that this integer of the claim is also disclosed in the Figure 9 embodiment.

273. It follows that Kiliccote does not anticipate claims 1 and 7 because it does not disclose transmission of a first message to a first server apparatus where that message includes a first identifier identifying the device or user of the device.

274. For completeness, and in case this matter goes further, I should also deal briefly with the argument in respect of the Defendants' construction. This was based on the disclosure in relation to Figure 3, where there is express disclosure that the server is configured to present the image to the user via a computer (col 3 lines 16-17). As I noted above, there is also this disclosure in the context of the Figure 9 embodiment. However, this makes no difference to my conclusion that Kiliccote does not anticipate claims 1 and 7, since the integer that is missing is not one which turns on this issue of construction in any event.

Obviousness – general principles

275. I have set out the relevant principles in the context of Schmidt, above.

Obviousness – argument and analysis

276. I can deal with this briefly, as both the evidence and the argument relating to this attack were very limited. As regards the evidence, Dr Berisso undertook a Pozzoli type analysis in his first report in respect of each integer of claim 1, saying whether he thought it was disclosed or obvious. However, I had difficulties with his evidence as he relied on different embodiments for the disclosure of different integers. I do not think that this is a legitimate approach for obviousness anymore than it is for anticipation.

277. Perhaps in recognition of that problem, the Defendants limited their written and oral arguments to the Figure 9 embodiment, although most of the arguments were

focused on the anticipation attack, and I was not addressed in any detail about the obviousness case separately. The Defendants' main point was to refer to what Prof Martin had said in chief, where he accepted that the differences he perceived between Kiliccote and the Patent were obvious except the requirement (on the Claimant's construction) that the encoded information is displayed on a sign which is static (i.e. non-electronic and does not change between transactions). As noted above, in cross-examination he accepted that a static sign was disclosed in the Figure 9 embodiment.

278. In the circumstances, I can see why the Defendants did not spend much time on this part of their case. However, despite what Prof Martin said in his written evidence, in my judgment the Defendants have not discharged the evidential burden in respect of this attack. First, neither expert addressed the Figure 9 embodiment in writing by reference to the integers of the claim. Second, whilst the Defendants' counsel addressed some of the integers with Prof Martin in cross-examination, she did not address them all. I agree with the Claimant that the relevant questions were not put to the Professor. In particular, counsel for the Defendants did not put to him that it would be obvious to the skilled reader implementing the third-party server/printed sign variant of Figure 9 to include a first identifier identifying the device or user of the device in the message sent from the secure device to the server. As a result, there was no evidence to support this part of the Defendants' case and I reject the attack of obviousness over Kiliccote.

INSUFFICIENCY

279. The Defendants attacked the Patent for uncertainty insufficiency. This is a concept which has recently been addressed by the Court of Appeal in *Anan Kasei v Neochemicals and Oxides* [2019] EWCA Civ 1646 per Floyd LJ at [22]-[25] and Lewison LJ at [99]-[101]. As Lewison LJ said:

> 99. A patent is personal property, without being a chose in action. We know that because section 30 (1) of the Patents Act 1977 tells us so. The essence of a right of property is that it distinguishes between what is mine and what is not mine. So there needs to be a boundary. If someone crosses the boundary, he invades my property right. The function of the claims is to delineate that boundary. As Lord Russell put it in *Electrical & Musical Industries v Lissen Ltd* (1939) 56 RPC 23, 39: "The function of the claims is to define clearly and with precision the monopoly claimed, so that others may know the exact boundary of the area within which they will be trespassers."

> 100. In the case of an invention which, ex hypothesi, is new it may not be easy to delineate the boundary with precision. In the same way as a conveyance of land may not tell you precisely where the boundary is, with the result that any dispute may have to be resolved by looking at topological features on the ground, so the boundaries of an invention may have to be determined as a matter of interpretation in the light of the common general knowledge that the skilled person would possess. But once that exercise has been carried

out (these days including the possibility of equivalents), the court will be able to answer the question whether someone has crossed the boundary "yes" or "no". That, I think, is what Lord Hoffmann meant in *Kirin-Amgen Inc v Hoechst Marion Roussel Ltd* [2004] UKHL 46, [2005] RPC 9 at [126] by a "fuzzy boundary" (a phrase which is now part of the jargon of patent lawyers). The boundary may be fuzzy, but it is still a boundary.

101. In my judgment [counsel for the Defendants] was right to submit that there is a difference between a fuzzy boundary in that sense, and a boundary whose location is impossible to ascertain. It may be impossible to ascertain because it is described in meaningless terms (the famous example of Pinocchio units given by Jacob J in *Milliken Denmark AS v Walk Off Mats Ltd* [1996] FSR 292); or because the patent does not explain how to decide where the boundary is (as in Kirin Amgen itself). Patent lawyers have traditionally called this "ambiguity" but I do not think that that expression is accurate. Something is ambiguous when it is capable of having two (or more) meanings, and ultimately the court will be able to decide which of them is the correct meaning. Rather, in my judgment, the issue here is that of uncertainty. If the court cannot ascertain the boundary, having used all the interpretative tools at its disposal, it must conclude that the specification does not disclose the invention clearly enough and completely enough for it to be performed by a person skilled in the art.

280. The attack was only made on the Claimant's construction (which I have largely accepted). The Defendants argued that, based on that construction, the Patent does not teach the reader how they can ascertain whether a sign is sufficiently unchanging to fall within the scope of the claims. They suggested that the argument was reinforced by the Claimant's acceptance that the sign could be replaced from time to time.

281. However, the Claimant submitted that there was a difference between the inherent nature of a printed sign, being one that cannot change, and the fact that the sign can physically be replaced with another one. Its construction was limited to the former situation, which did not create any uncertainty.

282. I agree with the Claimant on this issue. I do not think that the scope of the claim is uncertain. To the contrary, the boundary is clear: the sign must be one which does not change once it has been created.

283. Further or alternatively, the Defendants argued that if the sign is required to be "geographically proximate" to the electronic apparatus to fall within the scope of the claims, the Patent does not teach the reader how to determine whether that requirement has been met. This was a defensive point, which arose to counter the way in which the Claimant argued the case in respect of Kiliccote. As noted above, the Claimant had argued that the printed sign in Kiliccote was not sufficiently proximate to the merchant's server for them to comprise the computing apparatus of the claim. I have rejected that argument and this

construction, so this point does not arise. However, if I am wrong, I agree with the Claimant that if the sign of the claim was required to be geographically proximate to the electronic apparatus, that would create a "fuzzy boundary" but would not make the claim uncertain.

284. Accordingly, I reject the attacks on the Patent in respect of insufficiency.

INFRINGEMENT

285. The allegation of infringement relates to the Defendants' payment system called the Shell Mobile Payment System. In summary, the system is based on the "Fill Up & Go" option within the Shell Motorist application. The user must download the app onto their phone and register with the service in advance, including with a payment method. Thereafter, when the user wants to fill up at a Shell service station, they use the app to scan the QR code displayed at the pump. They can then fill up their car with fuel as normal. Once finished, the app will confirm payment.

286. There are three iterations of the Shell system that are in issue. The Claimant alleged infringement of claims 1 and 7 in respect of all of them; claims 2 and 8 are not in issue because decoding in the Shell system takes place by the mobile phone and not at the server. There is a fourth "modern" iteration which is accepted not to infringe.

287. The three iterations in issue all employ a static placard displaying a QR code (albeit that the QR code is only used in the second and third iterations when geolocation or manual input are not used). The QR code is placed on top of the pump or on a structural pillar.

288. The Defendants provided a PPD which describes the Shell system in 18 steps. For the purposes of infringement, the steps that matter are Step 3 and Step 7.

289. In respect of the first iteration, Steps 1 – 3 describe the process by which the user logs on to the app. As part of this logon process, at Step 3 the user's credentials are sent to the Shell backend server (Mobile Payment Platform or MPP). The server checks the credentials against the database. Assuming the user is successfully validated, the server generates a digital hash value and sends it back to the user's app. According to the PPD, this is a "unique identifier" associated with that user. It is re-transmitted with every interaction that the user has with the server during that transaction and allows the user to interact with the MPP without having to sign in again.

290. Step 6 is when the user scans the QR code and the app processes it to extract (i.e. decode) the information. Subsequently at Step 7, the app sends a message to the MPP containing, among other things, the site and pump identifiers (which were decoded from the QR code at Step 6) and the digital hash value.

291. By contrast, with the second and third iteration, at Step 3 the user credentials are sent to a different server (CIPM). Assuming the user is successfully validated, that server provides the user with an access token. This has the same function as

the digital hash value, i.e. it avoids the need for the user to sign in again. Thereafter at Step 7 the first message is sent to the MPP server (as with the first iteration), but the parameters sent include the user access token instead of the digital hash value and this is checked with the CIPM and not the MPP.

292. The Defendants argued that there was no infringement by reference to the following points.

293. First, they contended that the QR code displayed on a static placard is not a "sign" within the meaning of claim 1. This turns on the construction of "which is displayed on a display of computing apparatus… wherein the display is a sign" which I have decided in the Claimant's favour. It follows that the Shell system satisfies this integer of claim 1. This applies to all three iterations.

294. Second, the Defendants argued that the message sent at Step 3 is the first message within the meaning of claim 1, and that since it does not comprise decoded information, it does not satisfy the requirements of the claim. This turns on the construction of "first message" which I have also decided in the Claimant's favour. It follows that just because the message sent at Step 3 is the first message in time, that does not preclude the message sent at Step 7 from being the first message within the meaning of the claim.

295. Third, the Defendants argued that the message sent at Step 7 did not satisfy the requirements of the claim that the "first message" includes "a first identifier identifying the device or user of the device". In support of this argument, they relied on three aspects of Prof Martin's evidence, as follows:

    i)   He said in chief that the digital hash value is only indirectly (rather than explicitly) an identifier of the user.

    ii) He agreed in cross-examination that the digital hash value was a session identifier which would change if the user went to a different pump.

    iii) He also said in cross-examination that he would expect the digital hash value to come from a number of inputs and would likely contain the user credentials, but he did not have enough evidence to say for certain.

296. The first point of evidence is only relevant if the claim requires the first identifier to be one that directly (or explicitly) identifies the user or device. However, I do not think that the claim is limited in that way. There is nothing in the language of the claim to support that construction; nor is it consistent with the teaching in the Patent or the purpose of the invention. The second point of evidence is correct as far as it goes, but ignores the fact that Prof Martin stressed that even if the digital hash value was an identifier, it still identified the user (albeit indirectly) and that they were registered to use the service. The third point does not seem to take the debate any further forward, since the upshot of this evidence is that, on the balance of probabilities, the digital hash value contains the user credentials. This will necessarily serve to identify the user.

297. It follows that the Shell system also satisfies this integer of claim 1, at least for the first iteration.

298. However, there is an additional argument in respect of the second and third iteration, which relates to whether the CIPM or the MPP is the "first server" within the meaning of the claim. As noted above, with these subsequent iterations of the Shell system, the MPP is used at Step 7 but the user token which is sent as part of the first message is checked with the CIPM. In other words, two servers are used to achieve what is done with one server in the claim. Moreover, the claim requires the first message to be sent to the first server and for the first server, upon receiving the first message, to establish the identity of the user. In the second and third iterations the server that receives the first message (MPP) is not the same as the server that establishes the identity of the user (CIPM). It follows that the second and third iterations of the Shell system do not fall within the scope of the claim because the first server of the claim (MPP) is not the server that establishes the identity of the user of the device, contrary to the requirements of the claim.

299. As a result, in my judgment the first iteration of the Shell system would infringe the Patent (if it were valid) on the Claimant's construction of "wherein the display is a sign". By contrast, the second and third iterations of the Shell system would not.

CONCLUSIONS

300. I have largely accepted the Claimant's construction of the Patent. On this construction:

    i)   claims 1, 2, 7 and 8 of the Patent are invalid for added matter;

    ii)   claims 1, 2, 7 and 8 of the Patent are invalid on the basis of extended protection;

    iii)   claims 1, 2, 7 and 8 of the Patent are obvious over Schmidt;

    iv)   if the validity of the Patent had been upheld, the first iteration of the Shell system would have amounted to an infringement of claims 1 and 7, but the second and third iterations would not.

301. However, if am wrong on construction, and the Defendants' construction is the right one:

    i)   it is accepted that claims 1 and 7 of the Patent are anticipated by Schmidt;

    ii)   claims 2 and 8 of the Patent are also anticipated by Schmidt;

    iii)   claims 1, 2, 7 and 8 of the Patent are obvious over Schmidt;

    iv)   it is accepted that the Patent is not infringed.

Annex – Relevant Figures from Kiliccote

FIG. 1

FIG. 2

FIG. 3

FIG. 9

FIG. 9
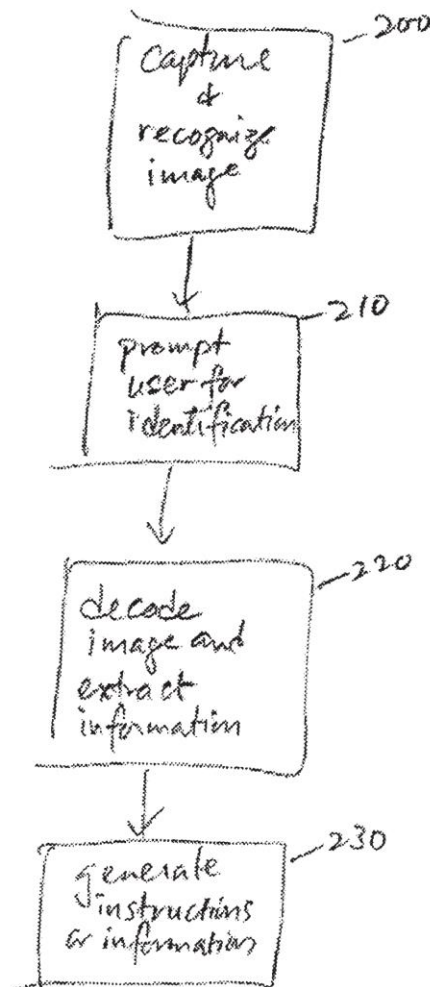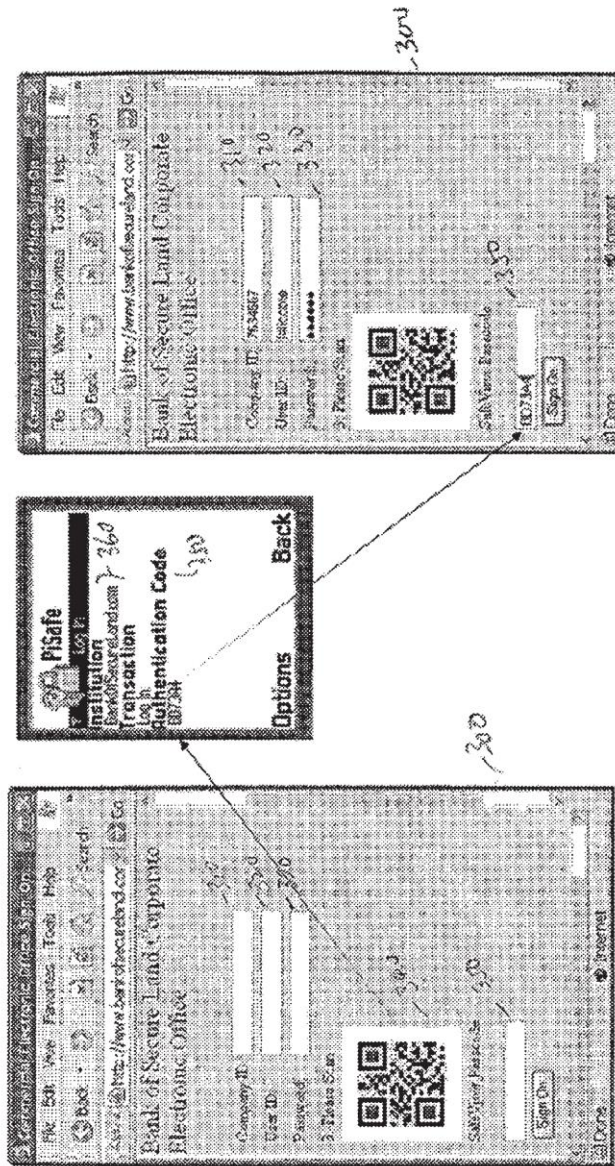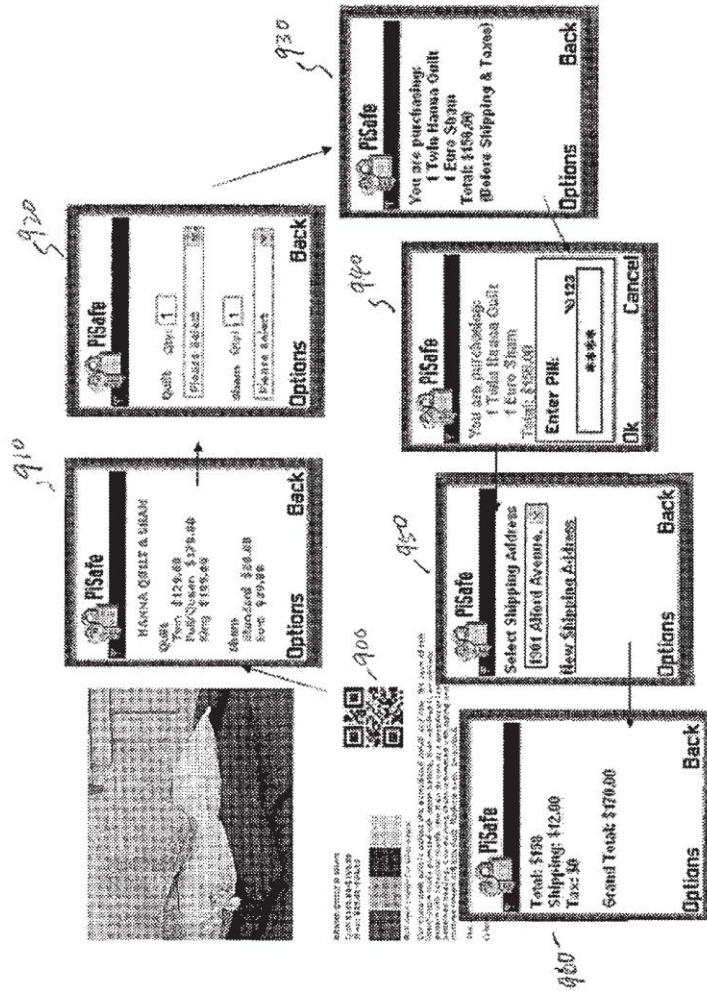*(Continued)*

66