Neutral Citation Number: [2019] EWHC 1302 (IPEC)

Case No: IP-2017-000169

IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
INTELLECTUAL PROPERTY ENTERPRISE COURT

Royal Courts of Justice, Rolls Building
Fetter Lane, London, EC4A 1NL

Date: 22/05/2019

Before :

HIS HONOUR JUDGE HACON

- -

Between :

PROSYSCOR LIMITED	**Claimant**
- and -	
(1) NETSWEEPER INC.	
(2) NETSWEEPER (BARBADOS) INC.	
(3) JEREMY ERB	**Defendants**

- -
- -

James St Ville (instructed by **SA Law LLP**) for the **Claimant**
Hugo Cuddigan QC and **Chris Aikens** (instructed by **Haseltine Lake Kempner LLP**) for the **Defendants**

Hearing dates: 9-10 April 2019

- -

Approved Judgment

I direct that pursuant to CPR PD 39A para 6.1 no official shorthand note shall be taken of this Judgment and that copies of this version as handed down may be treated as authentic.

.....

HIS HONOUR JUDGE HACON

Judge Hacon :

Introduction

1. This is a dispute about the ownership of an international patent application and national and regional applications derived from it. The invention claimed is a method of discriminating between requests to access a website.

2. Widespread use of the internet began in the 1990s. Since then a necessary tool for both users and website operators has been the ability to block websites. For instance users wish to protect children from inappropriate material and operators want to ensure that only paying subscribers have access to their website.

3. Alternative means have been developed to achieve the required selective blocking, initially by reference to a computer's internet protocol address ('IP address'). Users and/or website operators could prevent a computer at an identified IP address gaining access to selected websites. However, single IP addresses increasingly came to be used by more than one computer. By way of example, schools came to use one IP address so that all the school's computers could be protected by a single firewall. Yet they still wanted students to have more limited access to websites than the staff and some of the staff may have had subscriptions to websites behind a paywall. There arose a need for a system whereby individuals could be identified and authorised to use a website independently of their IP address.

4. PCT Application No. WO 2013/177687 A1 ('the PCT Application') claims an invention which meets this need. It is owned by the second claimant, a Barbados company set up to hold IP rights controlled by the Netsweeper group of companies. The first defendant is the Canadian parent of the group. I will refer to them collectively as 'Netsweeper'. The third defendant, Mr Erb, is an employee of Netsweeper and is identified as the inventor in the PCT Application.

5. The claimant ('Prosyscor') is a UK company set up by Bradley Kite as a vehicle for the development and commercialisation of software written by him called 'Authent'. Authent provides a means to discriminate between computers that share a single IP address when blocking access to websites.

6. Mr Kite is a former employee of Netsweeper and was for a time following his employment a consultant to the group. There was disagreement in the evidence as to whether he was employed by the Canadian parent or by a UK subsidiary, now dissolved, but it was not important.

7. Mr Kite says that while he was employed by Netsweeper he developed the invention claimed in the PCT Application in circumstances such that he, not Netsweeper, is entitled to the rights in the invention. Through his company Prosyscor he claims ownership of the PCT Application and all applications derived from it. Mr Kite also alleges that during his period of consultancy he disclosed in confidence information relating to his invention to Mr Erb and a colleague of Mr Erb's at Netsweeper. He says that in breach of confidence the information has been exploited by Netsweeper.

8. Netsweeper accepted that Mr Kite should be named as joint inventor along with Mr Erb on the PCT Application and any patent applications and granted patents derived from it. Mr Erb is said by Netsweeper to retain his status as an inventor because part of the invention consists of Mr Erb's improvement on Mr Kite's idea. Netsweeper also argue that naming Mr Kite an inventor leaves ownership unaffected because Mr Kite's contribution was made while he was Netsweeper's employee, or alternatively was made under a contact the terms of which award to Netsweeper the ownership of the rights derived from Mr Kite's work.

9. Mr Erb was joined as the third defendant solely because of his status as named inventor on the PCT Application. Mr Erb gave evidence at trial and played a significant role in the events leading to the litigation, but not a major role as a party. I will treat Netsweeper as if they were the only defendants.

10. James St Ville appeared for Prosyscor, Hugo Cuddigan QC and Chris Aikens for Netsweeper.

The reference

11. On 25 January 2018 Prosyscor made a reference to the Comptroller under section 12 of the Patents Act 1977 ('the 1977 Act') in relation to the PCT Application. In a written decision dated 25 May 2018 the Comptroller declined jurisdiction in favour of this court.

The issues

12. Before the trial the parties helpfully narrowed the issues between them and during the trial they narrowed further. They are as follows:

Inventorship

(1) What are the inventive concepts disclosed in the PCT Application?

(2) Which inventive concept(s) were devised by Mr Kite and which (if any) by Mr Erb?

Entitlement

(3) Were the inventive concept(s) devised by Mr Kite made in the course of his normal duties as an employee of Netsweeper?

(4) In so far as Mr Kite devised the inventive concept(s) after the termination of his employment on 1 September 2010, were the rights to the invention governed by the Ancillary Agreement of 6 January 2009?

Breach of confidence

(5) What confidential information was disclosed to Netsweeper pursuant to the Confidentiality Agreement of 7 June 2011?

(6) Was anything disclosed beyond what had been disclosed in the First and Second Intranet Posts?

(7) Have Netsweeper made use of any information so disclosed?

The witnesses

13. Mr Kite and Mr Erb were both cross-examined, as was Lou Erdelyi, Chief Technology Officer of Netsweeper. I found all three to be good witnesses. I think Mr Cuddigan was right to point out that Mr Kite's position as to when he devised an inventive concept changed during the course of these proceedings from a date after his employment by Netsweeper to a date during that employment. This was a significant shift and Mr Kite acknowledged it to be so during cross-examination. Fairly, in my view, Mr Cuddigan did not ask me to infer from this change of position that Mr Kite was to be treated as an unreliable witness. I do not believe he was, although it cast some doubt over the accuracy of Mr Kite's memory about dates.

14. There was a witness statement from Matthew Holt, who sold Netsweeper products in the UK and introduced Mr Kite to Netsweeper as a prospective employee. Mr Holt's evidenced was not challenged.

The law

The inventive concept

15. I recently considered the law on entitlement to a patent under an international convention in *BDI Holding GmbH v Argent Energy Ltd* [2019] EWHC 765 (IPEC), at [11]-[29], referring in particular to *Yeda Research and Development Co Ltd v Rhone-Poulenc Rorer International Holdings Inc* [2007] UKHL 43; [2008] RPC 1. Counsel both agreed with the law as stated in *BDI Holding*. I must identify the inventive concepts disclosed in the PCT Application and decide who devised them. The inventive concepts are to be identified by reading the document through the eyes of the skilled person. There was no material dispute between the parties regarding the attributes of the skilled person or the common general knowledge.

Entitlement

16. Section 39 of the Patents Act 1977 provides, so far as is relevant:

> ***39 Right to employees' inventions.***
>
> *(1) Notwithstanding anything in any rule of law, an invention made by an employee shall, as between him and his employer, be taken to belong to his employer for the purposes of this Act and all other purposes if –*
>
> > *(a) it was made in the course of the normal duties of the employee or in the course of duties falling outside his normal duties, but specifically assigned to him, and the circumstances in either case were such that an invention might reasonably be expected to result from the carrying out of his duties; or*
> >
> > *(b) the invention was made in the course of the duties of the employee and, at the time of making the invention, because of the nature of his duties and the particular responsibilities arising from the nature of his duties he had a special obligation to further the interests of the employer's undertaking.*

> *(2) Any other invention made by an employee shall, as between him and his employer, be taken for those purposes to belong to the employee.*

17. The sole issue between the parties in relation to s.39 was whether any invention made by Mr Kite during his employment was made in the normal course of his duties as an employee of Netsweeper within the meaning of s.39(1)(a). It was not argued that any invention had been made in the course of duties specifically assigned to Mr Kite. Nor was it in doubt that if made in the normal course of his duties, the circumstances were such that an invention might reasonably be expected to result from the carrying out of those duties.

18. In *LIFFE Administration and Management v Pavel Pinkava* [2007] EWCA Civ 217; [2007] RPC 30, Dr Pinkava had been employed by LIFFE, the operator of the London Futures Exchange, as a manager in its Interest Rate Management Team. He devised a system and related inventions which permitted the trading on an electronic exchange of financial instruments not previously so traded. Dr Pinkava filed four applications for US patents. LIFFE claimed that it was entitled to the applications. One of the issues was whether Dr Pinkava had made the inventions in the course of his normal duties as an employee.

19. The Chancellor (Sir Andrew Morritt) said:

> "[56] The only contrast drawn by s.39 between one sort of duty and another is to be found in the alternatives 'normal' and 'specifically assigned'. Unless the invention was made in the course of a duty falling within one or other description, which are in terms mutually exclusive, s.39(1) cannot apply and the invention will belong to the employee. It may be that there is a third category of duty, such as that adverted to by the Banks Committee in para.469 of their report (see [39] above), but it is unnecessary to decide the point because it is irrelevant. Further the emphasis is on a duty of the relevant description. The source of an employee's duty is primarily contractual, though some of the terms are implied by law, cf *Patchett v Stirling* (1955) 72 R.P.C. 50, 56 and 58. But the contract evolves in the course of time such that, in my view, it is unsafe to have regard only to the terms contained in an initial written contract of employment. The actions of employee and employer in performance of the contract may give rise to an expansion or contraction of the duties initially undertaken by a continuous process of subtle variation. I do not think that any extra or different duties so undertaken should be regarded only as duties 'specifically assigned'. It is quite possible for them, in the course of time, to have become 'normal'.
>
> [57] The suggestion that what is 'normal' is to be ascertained by reference to some other standard such as 'ordinary', 'day to day' or 'primary' must also, in my view, be rejected. Parliament has chosen the word 'normal'. It is not for the courts to substitute for that ordinary English word some other test which may or may not be quite the same. It is for the courts to apply the test selected by Parliament in accordance with its normal meaning. Thus I agree with Falconer J. in *Harris' Patent* [1985] R.P.C. 19, 28 that the cases decided before the enactment of s.39 can only be guidance in relation to the assessment of an employee's duties in the circumstances of that case. For my part I doubt if they are helpful in even that limited context.

> [58] It is not in doubt that the duties of an employee may evolve in the course of time, see *Armstrong Whitworth Rolls Ltd v Mustard* [1971] 1 A.E.R. 598 and *Carmichael v National Power Plc* [2000] I.R.L.R. 43, [33]. Accordingly, I agree with counsel for LIFFE at least to the extent of examining the judgment of Kitchin J. on this part of the case to see if he did pay sufficient regard to the possibility of the evolution of duties as normal over and above those set out in the initial contract of employment. …"

20. Longmore LJ agreed with the Chancellor. Jacob LJ did too, save with regard to one matter which is not in issue here. Jacob LJ also considered 'normal duties'. He pointed out first that s.42(2) of the 1977 Act overrides any term in a contract of employment which limits an employee's rights to his invention, so that that such rights are governed solely by s.39(1) and (2). Jacob LJ continued:

> "[97] It is against that background that one comes to s.39(1). Both (a) and (b) focus on the employee's duties ('normal' or 'specifically assigned' for (a) and a 'special obligation to further the interests of the employer' for (b)). How then does one ascertain the nature of the employee's duties? 'Duty' is the language of obligation. As between the employer and employee the primary source of a duty are the terms of the contract. What is it that he is employed to do must be the key question. That is not the same thing as was suggested by Mr Tritton – what is his day-to-day work? Take for instance a research chemist working on a cancer cure for the last 10 years. Suppose he came up with a cure for arthritis. He could not seriously contend that he owned the invention because he was day-to-day working on a cancer cure. His duty as a research chemist is clearly wider than his day-to-day work.
>
> [98] On the other hand the contract cannot be sole arbiter of the duty. Otherwise employers would be able to include overbroad duties in contract terms and s.42(2) would not operate to make the contract unenforceable. As I have noted, that was specifically a matter of concern to the Banks Committee. Section 42(2) will have effect to deal with overstated duties. The 'duties' of s.39(1) are determined realistically.
>
> [99] Since one cannot go by the contract alone I do not think one can be too precise about how the duty is to be ascertained. The contract and the general nature of the job both call for examination. It is not possible to be too analytical about this. In the end one is asking whether the employee is employed to try to innovate and, if he is, what general sort of areas his innovation duties cover. It is here that I think Kitchin J. got too far into the detail of Dr Pinkava's day-to-day work, accepting that he was under a duty to innovate new types of future of a conventional kind but not other types of product which would be of commercial interest to LIFFE.
>
> [100] Clearly another factor relevant to the determination of duties is the extent to which the common law imposes a duty of confidence on the employee. Section 42(3) makes it clear that Parliament was not intending to abrogate this duty in relation to employee inventions. So if in the course of his work an employee comes up with an idea which the common law would require him to hold as confidential to his employer, that will be covered by s.39. Any other conclusion leads to the absurd result that an invention would belong to the

> employee and yet he would owe a duty of confidence to his employer. Parliament cannot have intended such a stalemate. It follows that to some extent at least, although s.39(1) is a complete code, it lets the common law back in via the concept of 'duty'.
>
> [101] The section provides that the invention must be made 'in the course' of the employee's duties. This clearly draws on the well-known common law concept of 'in the course of employment'. The classic contrast is 'a frolic of his own'. In practice once the duties are ascertained this requirement should cause little difficulty."

21. I draw from these judgments the following principles relevant to this case:

(1) An invention made by an employee will belong to him unless it was made in the course of the categories of duty expressly identified in s.39(1): 'normal duties' or 'duties specifically assigned to him' under s.39(1)(a), or duties of a nature such that the employee has 'a special obligation to further the interests of the employer's undertaking' under s.39(1)(b).

(2) The two categories under s.39(1)(a) are mutually exclusive.

(3) The meaning of 'normal duties' in s.39(1)(a) is not to be resolved by reference to characterisations such as 'ordinary', 'day to day' or 'primary' duties.

(4) The starting point in defining normal duties is the contract of employment; having considered the terms of the contract one must ask: what was the employee employed to do?

(5) However, the contract of employment is not the sole arbiter of normal duties. The overall question is whether the employee was employed to try to innovate and if so, what general sort of areas his innovation duties covered at the relevant time, i.e. the date on which the invention was made.

(6) The duties of an employee may evolve over the course of time. The actions of employee and employer may give rise to an expansion or contraction of the duties initially undertaken and/or those specified in the contract of employment, so that they become (or cease to be) normal duties.

(7) The duty of confidence owed by an employee to an employer may provide a guide to the scope of his normal duties. If the circumstances are such that the employee would owe an equitable duty of confidence to his employer with regard to the invention, the invention will belong to the employer pursuant to s.39.

(8) An invention is made 'in the course of' an employee's normal duties under s.39(1)(a) generally in contradistinction to being made in a frolic of his own.

Technical background

Internet browser

22. An individual using the internet will commonly access content by means of an internet browser, such as Internet Explorer or Chrome. This consists of software loaded on to the individual's computer. The individual types a uniform resource locator (URL), commonly known as a web address, into the browser which causes a request to be transmitted to the website. Alternatively, a word is typed into a search engine provided by the browser which generates alternative URLs and by clicking on one of them, the individual sends the request.

23. All websites consist of pages, media and other files which together make up the website stored on a web server. A web server is a large computer connected to the internet. The browser communicates with the website via an internet service provider (ISP). The website responds to the request sent by the individual by sending data back to his or her computer via the ISP. In the simplest case, the individual's computer screen then displays the pages of the website.

Cookies

24. Cookies are pieces of text transmitted by a website. They can be stored on the hard disk of a computer. The presence of a stored cookie on a computer can be used, among other things, to signal that the relevant website may be accessed by that computer.

Authentication and filtering access to a website

25. There are various ways to discriminate between requests for access to a website. In a simple example the website will have a default policy of denying access upon request, sending back a 'deny' page to the computer which sent the request. However the page will provide for the possibility of entering a username and/or a password. If the website recognises the username and password from its database, the person sending the request is 'authenticated' and the website content is sent. If not, the deny page remains in place.

A proxy

26. A proxy is a device, another computer, located between the user's computer and websites. The proxy modifies, filters or logs the user's request to access websites. It can also store copies of web pages commonly requested to speed up retrieval.

27. When performing a filtering function, a request from the proxy's client computer can be checked against a policy stored in the proxy. If the request is contrary to the policy, it is blocked and never makes it to the website. If sanctioned by the policy, the request is allowed to proceed.

The PCT Application

28. The PCT Application explains that in the past proxies have been used to enforce a policy for access to websites. However, placing a proxy between the requesting computer and the requested content can create a bottleneck, in that allowed requests may not be fulfilled quickly enough to meet demand. The PCT Application goes on to say that administering proxies can be onerous, particularly in large organisations.

29. The invention claimed provides a means of filtering requests for access to websites without the need of a proxy.

Claims 1 and 11

Claim 1

30. Although they do not correspond exactly, claim 1 can be visualised by reference to figure 4:

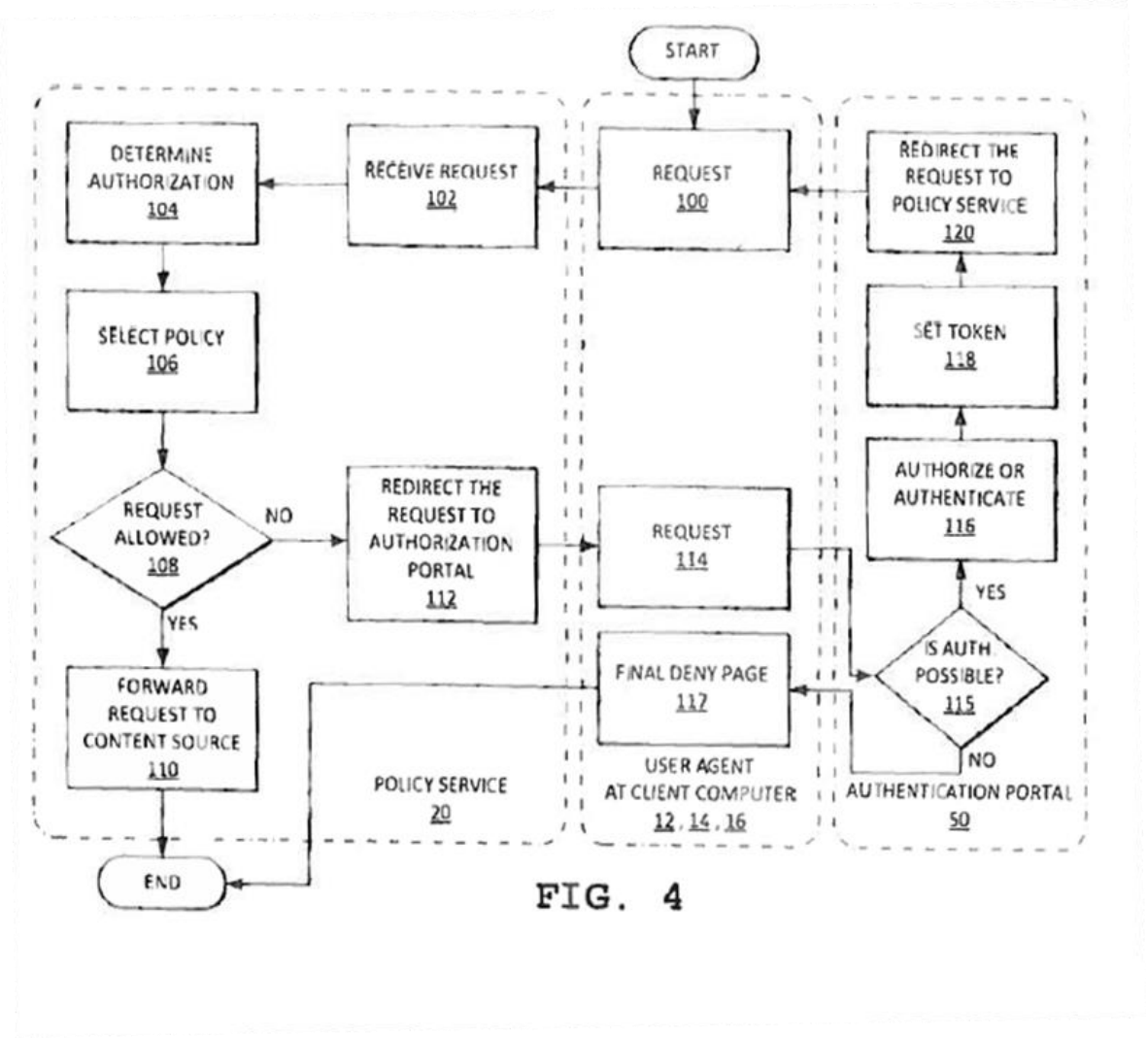

FIG. 4

31. There are three parts to the system which performs the method of claim 1. The dotted lines in figure 4 distinguish them. First there is the user's computer (the user is referred to as the 'user agent'), shown in the centre of figure 4. Secondly the 'policy service' which is a computer configured to apply the policy which discriminates one user agent from another when attempting to access to a website, shown on the left. Thirdly, on the right, there is the 'authentication portal' which can identify the user agent so that the policy service may then allow access to a requested website.

32. Claim 1 is as follows, with numbers in square brackets added by me to correspond with the numbers in figure 4:

> "A method of applying network resource access policy, the method comprising:
>
> receiving from a user agent a request [102] for a remote network resource;

> obtaining from the request authorization data specific to the remote network resource when the request contains the authorization data [104];
>
> determining a resource access policy for the request, including using the authorization data, if obtained, to determine the resource access policy for the request [106];
>
> applying the resource access policy [108] to allow or deny access by the user agent to the remote network resource;
>
> when denying access to the remote network resource, redirecting the user agent to an authorization portal [112, 114];
>
> after authorization by the authorization portal [115-116], receiving from the user agent an authorized request [100] for the remote network resource, the authorized request including an authorization token [118]; and
>
> in response to receiving the authorized request including the authorization token [102], storing the authorization data specific to the remote network resource at the user agent and redirecting the user agent to the remote network resource to cause the user agent to make another request for the remote network resource [104, 106, 108 and 110]."

Claim 11

33. Claim 11 is:

> "11. A system for applying network resource access policy, the system comprising:
>
> a filter configured to apply resource access policy to a request from a user agent for access to a remote network resource by redirecting the user agent to an authorization portal when denying the request for the remote network resource, the filter further configured to respond to an authorized request having an authorization token by storing authorization data at the user agent and redirecting user the agent [sic] to the requested network resource; and
>
> a policy server configured to determine resource access policy based on the request as provided by the filter and further based on any authorization data accompanying the request."

34. The significant feature of claim 11 is a filter which is separate from the policy server. The two may be separately located. The filtering and the application of the policy are thus done independently.

35. Claim 11 is not dependent on claim 1, so need not incorporate exactly the steps of claim 1. Figure 5 illustrates how the claim 11 system could typically work, demonstrating the increased number of steps when compared with claim 1:

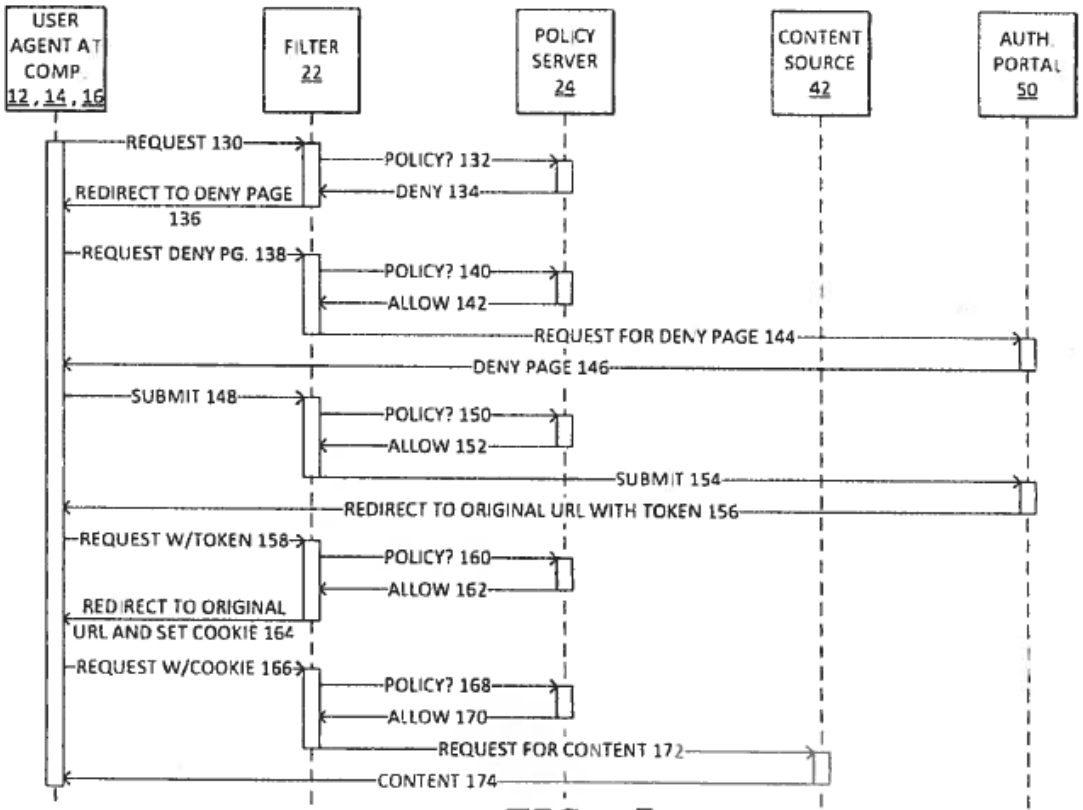

FIG. 5

36. Figure 5 can be explained as follows by reference to the numbers in the diagram:

(1) An individual (user agent) makes a request [130] for access to a website (content source). The request is intercepted by a filter [22].

(2) The filter requests [132] a policy decision from a policy server [24], a computer programmed to apply the desired policy for access to websites.

(3) The policy server's first response [134] is a decision to deny access.

(4) There is an authorization portal [50], a computer which can authorise a request for access to a website, but which also hosts a deny page. The decision from the policy server to deny [134] causes the filter to instruct the user agent's computer to redirect [136] to the authorization portal's deny page.

(5) The user agent's computer sends a request [138] to the filter which, having had the request approved [140 & 142] by the policy server, requests [144] the deny page from the authorization portal.

(6) The deny page is sent [146] to the user agent's computer, i.e. the screen displays to the user agent a page with the message that access to the website has been denied. The deny page also contains a section permitting the user agent to type in their credentials, typically a username and password. If these are entered, the request is submitted again [148 & 150] to the policy server via the filter. The

policy server submits [154] to the authorization portal a request for access to the website.

(7) The authorization portal responds by redirecting [156] the request back to the user agent's computer, together with an 'authorization token' which contains a unique identifier, corresponding to the credentials supplied by the user agent.

(8) The user agent's computer then sends a second request [158] to the filter, now with the authorization token.

(9) The filter passes [160] the request, along with the authorization token, to the policy server, which allows the request and passes it back [162] to the filter.

(10) The filter redirects [164] the request back to the user agent's computer together with a cookie injected by the filter, which contains authorization data.

(11) The request, now with the cookie, is submitted a third time [166] by the user agent's computer to the filter.

(12) The filter sends [168] the third request, with cookie, to the policy server. If the data in the cookie does not satisfy the policy, the policy server will respond by redirecting the user agent's computer to the deny page (as above).

(13) Alternatively if, as is shown in figure 5, the cookie data satisfies the policy, the policy server will direct [170] the filter to request content from the website ('the content source [42]).

(14) The filter requests [172] content from the website.

(15) The website then sends [174] the content to the user agent's computer.

The inventive concepts disclosed in the PCT Application

37. Netsweeper's case was that there were two inventive concepts defined by the entirety of claims 1 and 11. Prosyscor started with six inventive concepts but as argument developed Prosyscor also focussed on claims 1 and 11.

38. As I said in *Regen Lab SA v Estar Medical Ltd* [2019] EWHC 63 (Pat) (at [234]), it is generally both helpful and necessary to simplify the inventive concept as much as can accurately be done. Unless a patent claim is very succinct, the inventive concept is almost bound to be more confined than the totality of the claim. In the context of a dispute about entitlement to a patent, being precise about the inventive concept is likely to matter when it comes to identifying who devised it. Of course, stating an inventive concept may require that it is put into some sort of context so that it can be understood. But it should be possible to distinguish between the context and the concept.

39. In the present case neither side made any attempt to be precise. For reasons that will become apparent, it didn't matter. It is therefore not necessary for me to attempt to fillet out the inventive concepts contained in claims 1 and 11.

The devising of the inventive concepts

40. After Mr Kite left school he taught himself how to create computer programs and gained employment as a software developer. By 2008 he was working for a company called Synetrix Ltd. One of Synetrix's clients was Netsweeper. Netsweeper offered Mr Kite a job by a letter dated 26 September 2008, an offer made with Synetrix's knowledge and consent. The offer was accepted by Mr Kite. On 6 January 2009 Mr Kite started working at Netsweeper and on the same day he entered into a further written agreement with Netsweeper ('the Ancillary Agreement').

41. According to Mr Kite, in March 2009 he began to develop an idea of how to authenticate computer users independently of an IP address. He said that this was done in his own time, on his own equipment, as his own project.

42. On 30 March 2009 Mr Kite posted a summary of his authentication idea on an internal website used by Netsweeper ('the First Intranet Post'). The internal website was only accessible to Netsweeper staff. Mr Kite's idea included what was referred to as a 'pending pool'. The pending pool stored requests to use a website from users who had been authenticated by the authentication portal. It allowed authenticated users to continue to access the relevant website pending such time as a cookie could be set in the browser on their computer.

43. Later on 30 March 2009 there was a Skype conversation between Mr Erb and Mr Kite followed by an email sent to Mr Kite by Mr Erb. Mr Erb was enthusiastic about Mr Kite's idea but pointed out a difficulty: if the pending pool registered a request for a website which had been authenticated by one user, other unauthenticated users requesting the same website would be permitted access. Mr Erb suggested a solution, namely the authorization token idea (see steps (7) to (9) of the annotation of figure 5 above). Because this token worked by adding a message to the relevant URL, it was sometimes referred to as 'URL mangling'.

44. Mr Kite continued to work on the idea and on 21 August 2009 posted an amended summary on Netsweeper's internal website ('the Second Intranet Post'). This was further edited on 23 September 2009.

45. Despite Mr Erb's earlier enthusiasm, support for it from Netsweeper generally was limited.

46. In 2010 Mr Kite decided that he wanted to leave Netsweeper's employment. Netsweeper agreed and as of 1 September 2010 he became a consultant, working with Netsweeper under a new agreement ('the Consultancy Agreement').

47. Mr Kite continued work on his user authentication idea, creating new software to operate a system embodying the idea which he named 'Authent' in October 2010. In November 2010 Mr Kite engaged a firm of patent attorneys to draft a patent application claiming his Authent system. On 2 November 2010 Prosyscor was incorporated to market Authent.

48. Meanwhile, in the early part of 2011 Netsweeper began work on a system which came to be called 'Authenticated Override'. It was prompted by discussion with a potential customer, Education Network of America ('ENA'). ENA provided computer network services to schools in the United States. In time Authenticated Override became an

improved means of allowing varied levels of internet access to computers within a school using a single IP address.

49. According to Mr Kite, in May 2011 he realised that there was an opportunity to commercialise his Authent system through Netsweeper. There is no doubt that he and Netsweeper came to the view that there may be value in exchanging information about their respective proposed authentication systems. On 7 June 2011 Prosyscor and Netsweeper entered into a confidentiality agreement ('the Confidentiality Agreement') under which each was to disclose information to the other for evaluation only, under an obligation of confidence.

50. Mr Kite said that on the evening of the same day, 7 June 2011, there was a discussion by means of a Skype voice call. Mr Kite claimed that in the course of the call he disclosed confidential information about his Authent system to Mr Erb and Mr Graydon. Mr Erb said that no such call happened.

51. Netsweeper continued with the development of Authenticated Override. On 31 May and 4 June 2012 Netsweeper filed US provisional patent applications. These became priority documents for the PCT Application.

52. Mr Kite became aware of the PCT Application. On 30 August 2017 he assigned all his interest in the Authent system to Prosyscor and on 1 September 2017 Prosyscor started these proceedings.

The devisers of the inventive concepts

53. Prosyscor argued that Mr Kite devised the entirety of the inventive concept in claim 1. Its primary case in relation to claim 11 was that the claim contained nothing inventive. Alternatively, if it did, the inventive concept was devised by Mr Kite.

54. Netsweeper's case was that Mr Kite devised the main part of the claim 1 inventive concept, but Mr Erb devised an improvement. This was the idea of using an authentication token, which Mr Erb thought of and explained to Mr Kite in the skype call and email of 30 March 2009.

55. In cross-examination Mr Kite accepted that the authentication token, or URL mangling idea, came from Mr Erb. I find that Mr Erb is therefore joint inventor of claim 1.

56. I am not in a position to determine the inventiveness or otherwise of claim 11 – the idea of separating the filter from the policy server. I will consider who devised the inventive concept on the assumption, not a finding, that it exists.

57. Netsweeper said that the idea came from Mr Erb. That was Mr Erb's evidence and Mr Kite did not say otherwise. Mr St Ville argued that the separate filter was an implicit part of Mr Kite's Second Intranet Post and Mr Kite's draft patent application, the first draft of which was done in May 2011. This suggestion that Mr Kite had devised the separate filter idea and disclosed it to Mr Erb was raised for the first time in Mr St Ville's closing speech. It was not something Mr Kite had said and it was not pleaded by Prosyscor. It is not clear to me that the idea is implicit in the Second Intranet Post. To the extent that the idea formed part of Mr Kite's draft patent application, Mr Erb will not have seen that document, certainly not before Netsweeper's PCT Application

was created. It is possible that both gentlemen independently devised the idea. If that is what happened, the inventive concept of claim 11 is in the PCT Application because it was devised by Mr Erb.

58. I find that on the balance of probabilities, Mr Erb devised the claim 11 inventive concept.

Mr Kite's normal duties as Netsweeper's employee

59. The most important issue at trial was the scope of Mr Kite's normal duties. In this section of the judgment, 'the claim 1 inventive concept' will mean the claim 1 concept excluding Mr Erb's modification of using an authentication token.

60. As discussed above, the starting point is to consider the contract of employment and to ask what Mr Kite was employed to do. Mr Kite's terms of employment were set out in a letter dated 26 September 2008 from Netsweeper to him, signed by Mr Kite on 4 October 2008 and by Andrew Coutts, the President of Netsweeper two days later. It included this:

> "This letter is to confirm our offer of a position as a Senior Systems Engineer, reporting to Lou Erdelyi for pre-sales and post-sales support activities and to James Goruk for development activities; both of whom are based at Netsweeper Inc's Guelph, Ontario headquarters.
>
> …
>
> We have discussed and you will sign our Non Disclosure, Non-Compete Agreement where Netsweeper Inc. owns all materials developed by you.
>
> …
>
> You will be provided the necessary tools of your job, including work station, or lap top if needed, and approved expenses."

61. The Non-Disclosure, Non-Compete Agreement referred to was subsequently entered into on 6 January 2009. It was referred to at the trial as 'the Ancillary Agreement' and is discussed further below.

62. Attached to the contract was a document stating Mr Kite's roles and responsibilities, also signed by Mr Kite and Mr Coutts. The most relevant parts are:

> "In your role as Senior Systems Engineer, you will fill three central roles:
>
> - Development
> - Pre-sales support
> - Post-Sales and implementation support
>
> …
>
> <u>Development</u>

> As part of the development team, you will be responsible for the architecture, design and implementation and coding of key components and product capabilities for Netsweeper. This includes:
>
> - Intepreting and documenting product requirements in the Netsweeper wiki to create technical specifications for the work that will be performed.
> - Coding in accordance with the technical specifications
>   - Resultant code should provide inline documentation and be easily understood by other peer-level developers
>   - Resulting code should meet performance requirements
>   - Resulting code should be of high quality; i.e. few but preferably no defects and every effort should be made to ensure that there are no design defects.
> - Assisting QA in identifying QA requirements in terms of test plans, scripts, test data, etc.
> - Assist the documentation function of Netsweeper; identifying the doc requirements, reviewing documentation once completed and provided input to improve document quality.
> - Performing ongoing maintenance programming to correct any identified product defects and to optimize performance.
>
> In addition to the above, bring all of your ideas to the product management function within Netsweeper so that we can build the best products possible."

63. Mr Kite was a Systems Engineer employed, among things, to write software in order to create 'product capabilities for Netsweeper'. He was required to bring all his ideas to the product management team. On Mr Kite's own evidence, Netsweeper offered web-filtering software, something he knew before he joined. Mr Kite characterised Netsweeper's software as technology which control access to the internet in such a way as to make certain types of content unavailable to certain users. He also said in his witness statement that one of the main attractions of working for Netsweeper was that he would have the chance to do software development as part of his role.

64. I have no doubt that creating software of the type that allowed filtering access to websites in the manner claimed in claim 1 fell squarely within the normal duties of Mr Kite as contemplated by his contract of employment.

65. My view on Mr Kite's normal duties does not change if a wider view is taken and one asks whether he was employed to innovate and if so, what sort of areas his innovation duties covered at the time of his employment, when the claim 1 inventive concept was devised. Mr Kite was bound to innovate if he wrote software that gave rise to a method qualifying for patent protection. Such innovation was expected to be in the field of filtering access to websites – that was Netsweeper's core business.

66. Prosyscor's answer to this was that the work was done by Mr Kite at home in the evenings, in his own time, on his own computer. In my view, while the time and place of the devising of an inventive concept may be relevant to an assessment under s.39, they are secondary matters. In a case where there is otherwise doubt about whether an individual's acts were conducted in the course of his normal duties, the fact that they were done at home, outside office hours and using only tools owned by the individual may tip the assessment towards the view that the acts were not done in the course of his normal duties. But where, as here, they are very much the sort of acts which the individual was paid to carry out for the company, the fact that they were done at home makes no difference. Acts of a nature such as to be within the normal course of an employee's duties do not cease be so merely because the employee decides to carry out those normal duties at home and/or outside office hours and/or on his own equipment.

67. Supporting the characterisation of Mr Kite's work as falling within the course of his normal duties as an employee of Netsweeper is the fact that Mr Kite posted the claim 1 inventive concept on the Netsweeper intranet. He agreed in cross-examination that everything in the claim 1 method was disclosed in his Second Intranet Post of August 2009. Mr Kite accepted that this was a site accessed only by Netsweeper officers and employees because it contained Netsweeper's trade secrets. He explained that it was used as a useful tool for pooling ideas for development. Mr Kite signed Netsweeper's computer use document and accepted in cross-examination that by doing so he acknowledged that the company intranet was to be used only for Netsweeper business. Mr Kite further accepted that by posting his ideas on the Netsweeper intranet he had led Netsweeper to believe that these ideas – the claim 1 inventive concept – were to belong to Netsweeper.

68. In my view that last concession by Mr Kite was both honest and correct. I think the officers of Netsweeper would have been astonished to learn that ideas exchanged for discussion on its confidential internal website were anything other than ideas available for development by the company.

69. The argument advanced by Prosyscor in relation to the intranet posts was that such posting could not alter the status of the information. If the inventive concept was devised by Mr Kite outside the course of his normal duties, it belonged to him and that did not change just because he made Netsweeper aware of the concept. I agree that this is true as a matter of principle, but I think it misses the point. The relevance of Mr Kite posting the information on Netsweeper's intranet site was that it supports an already clear inference to be drawn from his contract of employment that devising the claim 1 concept was within the course of his normal duties.

70. The inference is also supported by the Ancillary Agreement which was signed on the first day of Mr Kite's employment. It included the following recital:

> "AND WHEREAS Employee has agreed to transfer and assign to [Netsweeper] all of his right, title and interest in and to all inventions, improvements, ideas, developments and all suggestions in Canada and any other country relative to the Employer products and technologies ("Confidential Information") all on terms as set out herein and for consideration set out herein;"

71. These are clauses 1 and 2:

> "l. Employee hereby agrees that any discoveries, ideas and suggestions, improvements or inventions of any character coming within the scope of the business of [Netsweeper] made or developed by Employee shall be for the benefit of the Corporation and shall be considered to have been made as if Employee were [an] employee of [Netsweeper] and shall immediately become the property of [Netsweeper].
>
> 2. Without limiting the generality of the foregoing Employee hereby transfers, sets over and assigns to [Netsweeper] his entire right, title and interest in and to any and all Trade marks, licenses and all inventions, improvements and discoveries in Canada and in any other country whatsoever and Employee hereby agrees to execute and deliver to [Netsweeper] any and all instruments and papers necessary or desirable to accomplish the assignment and transfer."

72. The Ancillary Agreement leaves no doubt that inventions by Mr Kite coming with the scope of Netsweeper's business were intended to belong to Netsweeper. No agreement between employer and employee can diminish the employee's rights under s.39 of the 1977 Act, see s.42. However, it is consistent with the view reached above regarding Mr Kite and Netsweeper's joint understanding of Mr Kite's normal duties under the terms of his employment contract.

73. On the present facts, I do not believe the question of whether Mr Kite owed a duty of confidence to Netsweeper adds much. I think he did owe such a duty in relation to the claim 1 concept but that is because I have formed the clear view that his job, among other things, was to come up with such concepts and therefore the claim 1 concept belonged to Netsweeper. Mr Kite was no more free to use or disclose that concept without Netsweeper's consent than was anyone else who came to learn of it as confidential information.

The effect of the Ancillary Agreement of 6 January 2009

74. The Ancillary Agreement, assuming that it continued to have effect after the end of Mr Kite's employment with Netsweeper, could make a difference only if Mr Kite had devised anything relevant after that. He did not.

Breach of confidence

75. As outlined above, in June 2011 Mr Kite and Netsweeper thought that there might be value in exchanging information about their respective progress on their projects. On 7 June 2011 they entered into the Confidentiality Agreement under which each was to disclose information to the other for evaluation only, under an obligation of confidence.

76. Prosyscor's case is that on the evening of 7 June 2011 there was a Skype voice call between him, Mr Erb and Andrew Graydon, the Chief Operating Officer at Netsweeper during which Mr Kite disclosed confidential information about his Authent system to Mr Erb and Mr Graydon. Mr Erb said that the call did not take place. Both Mr Kite and Mr Erb maintained their evidence on this in cross-examination.

77. I find it impossible to know whether the call did or did not happen and if it did, whether Mr Kite disclosed confidential information. However, I pressed Mr St Ville to be specific about what this confidential information was, over and above what had already

been disclosed by Mr Kite during the course of his employment. As with any other allegation of breach of confidence, it was essential for Prosyscor to identify clearly what the information in issue was. In the end Mr St Ville could only say that it was the knowledge that Mr Kite's Authent system worked.

78. Prosyscor's argument on breach of the Confidentiality Agreement therefore came to this. Netsweeper had lost faith in the filtering method which they had been developing, based on the claim 1 and 11 inventive concepts. Mr Kite's key information was that he had made it work. Armed with that information, Netsweeper went back to their work, which led to the development of their system.

79. I think that in theory confidential information could consist of nothing more than the information that a process can be made to work. However, a party alleging this faces a high evidential hurdle. First, the recipient of information that another party had succeeded in a project would almost certainly ask the donor what that other party had done to make the process work and thereby to explore what the recipient had not done or had done incorrectly. In most instances, a key piece of technical information would then be given and *that* would be the relevant confidential information, not the fact that the other party had succeeded. Only in unusual circumstances would the recipient, knowing only that the other party had succeeded, go back to exactly what they were doing before and find themselves able to make the system work. A party alleging breach of confidence would have to prove that these unusual circumstances had occurred.

80. Secondly, in order to prove a breach of confidence, it would have to be established that the information that the other party had succeeded in their project was by itself confidential. A party may have many reasons to announce openly, even to brag, that their project has been successful while disclosing nothing more about it. Such an announcement may well not be, of itself, confidential.

81. It was established that Netsweeper were having difficulties with their system but not that they had given up altogether. Their willingness to exchange information with Mr Kite suggests that they were still trying to succeed but thought that an exchange of information might help.

82. Assuming that on 7 June 2011 Mr Kite told Netsweeper that his Authent system worked, it was not shown that either party regarded this as confidential information or that a reasonable person in their shoes would have done so. Even if it had been, I am not satisfied that Netsweeper used this information in breach of confidence. The fact that they carried on with their project does not establish that the information was used. I find that Netsweeper are not in breach of the Confidentiality Agreement.

Conclusion

83. Netsweeper is entitled to ownership of the PCT Application and is not in breach of the Confidentiality Agreement with Prosyscor.