IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

WSOU INVESTMENTS, LLC D/B/A BRAZOS LICENSING AND DEVELOPMENT,	)	
Plaintiff,	)	
v.	)	Civil Action No. 21-1119-MN-CJB
NETGEAR, INC.,	)	
Defendant.	)	

REPORT AND RECOMMENDATION

At Wilmington this **14th day of July, 2022**:

As announced at the hearing on July 8, 2022, the Court HEREBY RECOMMENDS that Defendant Netgear, Inc.'s ("Defendant" or "Netgear") motion to dismiss (the "motion"), (D.I. 32), which argues that Plaintiff WSOU Investments, LLC d/b/a Brazos Licensing & Development's ("Plaintiff") asserted United States Patent No. 9,338,171 is directed to non-patent-eligible subject matter pursuant to 35 U.S.C. § 101 ("Section 101"), be DENIED.

Defendant's motion was fully briefed as of January 21, 2022, (D.I. 52), and the Court received further submissions regarding Section 101-related questions on July 1, 2022, (D.I. 76; D.I. 77). The Court carefully reviewed all submissions in connection with Defendant's motion, heard oral argument, and applied the relevant legal standards for review of this type of Section 101-related motion at the pleading stage, which it has previously set out in *Genedics, LLC v. Meta Co.*, Civil Action No. 17-1062-CJB, 2018 WL 3991474, at *2-5 (D. Del. Aug. 21, 2018).

The Court's Report and Recommendation is consistent with the bench ruling announced at the hearing on July 8, 2022,[1] pertinent excerpts of which follow:

> With that, let me move on to our first ca[se], and the first case is *WSOU Investments, LLC [d/b/a] Brazos Licensing [&] Development [vs.] Netgear, Inc*. It[is] Civil Action Number 21-1119-MN-CJB.
>
> For the reasons I will now state in this matter, I recommend that Netgear's motion to dismiss, which is pending before me, be denied.
>
> Here, the asserted relevant patent-in-suit at issue is Plaintiff's [U.S.] Patent Number 9,338,171, or the '171 patent. The patent is titled "Method and Apparatus for Controlling Access to Resources."
>
> At step one, the Court will treat claim 1 of the '171 patent, which is a method claim, as representative, as Defendant asserts that the claim is representative of the remainder of the asserted claims in the patent.
>
> Defendant argues that claim 1 is directed to the abstract idea of "controlling access to resources."
>
> Is "controlling access to resources" an abstract idea? The [United States Court of Appeals for the] Federal Circuit has repeatedly found that it is, such as in its decision in *Ericsson Inc. [vs.] TCL Communication Tech Holdings Limited*,[2] when the Federal Circuit said as much.
>
> The real dispute here at step one is whether claim 1 is in fact directed to this abstract idea. Plaintiff argues that it[is] not. Instead, it argues that the claims are directed to "distributed systems and methods that include wireless access points that further include an access control platform for security authentication that is based upon [(i)] social networking group designation and [(ii)] the limit of the number of users or traffic load information to prevent unauthorized access and performance

---

[1] (*See* D.I. 83)

[2] *Ericsson Inc. v. TCL Commc'n Tech Holdings Ltd.*, 955 F.3d 1317, 1326 (Fed. Cir. 2020).

degradation."[3] This is so, Plaintiff argues, because "[t]he claimed systems and methods reflect a patent-eligible improvement to computer functionality, such as network security authentication" and are not claims to an abstract idea.[4]

The "directed to" inquiry applies a stage-one filter to claims, considered in light of the specification, based on whether "'their character as a whole'" or their "focus" is directed to excluded subject matter.[5] As to how that inquiry should proceed, the Federal Circuit provided some guidance in *Internet Patents Corp. v. Active Network, Inc*.[6] There, in order to ascertain at step one whether the claims' "character as a whole" was directed to an abstract idea, the *Internet Patents* Court examined the specification of the patent at issue.[7] In doing so, it cited to what the patentee had described in the specification as "the innovation over the prior art" and "the essential, 'most important aspect'" of the patent.[8]

Here, the parties don't spend a lot of time in the briefing explaining how, when one looks to the content of claim 1 and the specification, one should determine what the claim is directed to. Nevertheless, the Court will focus in some detail here on that question.

On the one hand, as Defendant notes, the title of the patent, which is "Method and Apparatus for Controlling Access to Resources," helps its argument. That title makes it sound like the patent is focused simply on the general broad abstract idea posited by Defendant.

---

3 (D.I. 45 at 11)

4 (*Id*.)

5 *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335-36 (Fed. Cir. 2016) (quoting *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015)).

6 *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343 (Fed. Cir. 2015).

7 *Id.* at 1348.

8 *Id.* (citation omitted); *see also Genetic Techs. Ltd. v. Merial L.L.C.*, 818 F.3d 1369, 1375-76 (Fed. Cir. 2016) (assessing "the focus of the claimed advance over the prior art" in the step one inquiry).

Moreover, if one looked only at the Background section of the patent, it might also support Defendant's assertion. In column [1], line 14 to 30[] of that section, the patent explains how service providers want to provide a service that allows for the sharing of resources among users, such as allowing other users to be able to access a wireless access point when the users are within the range of the access point. The section also notes how "[j]uxtaposed with the ability to enable users to share resources is the need to maintain security with respect to the resources . . . without degradation of performance of the resources."[9] It notes that a user who shares a wireless access point among designated users may wish to maintain a certain level of both security and performance of the access point, but that the uses of security features may make "sharing the resources complex."[10]

Portions of column 4 of the patent expound on this problem. In column 4, lines 14 to 52, the patent explains that most providers of wireless access points at the time used password protection to prevent unauthorized people from connecting to an access point to the internet or to other network resources without permission; they also used this method to prevent such persons from eavesdropping on their permitted users who were using the access point. But the specification then notes how the static, password-based security protocol also created problems for service providers. More particularly, if the provider had given out passwords to all of its users, and if it later decided that it wanted to block one of those users from access, a new password had to be created and distributed to other authorized users, or "even more complex processes" had to be used.[11] This portion of column 4 also described another problem that providers were having in this sphere: namely that if the number of users associated with an access point got too large, there might be issues with "degradation of services[.]"[12]

This is all to say if you look only to the patent's title or to the portions of the patent that cite the *problem that the patent sets out to solve*, like the Background section and these portions of column

---

9 ('171 patent, col. 1:21-24)

10 (*Id.*, col. 1:29-30)

11 (*Id.*, col. 4:35)

12 (*Id.*, col. 4:40-41)

4, then you might conclude that claim 1 is simply directed to the broad concept of "controlling access to resources."

But in the Court's view, there are more persuasive reasons to conclude that the claim is not, in fact, directed to this general principle, and instead is directed to something other than that. For example:

As Plaintiff notes, large portions of columns 4 through 8 are not simply about "controlling access to resources" generally. Instead, they describe a proposed solution to these problems: a *more specific way* of controlling access to resources, namely doing so by utilizing social networking information associated with the users, and also by utilizing performance characteristics associated with resources (and, in the context of this patent, when I say "resources," that can be understood to be a reference to wireless access points.) For example, in column [4], line 53 to column 5, line 45, the patent explains that "[t]o address these problems," the claimed system and methods will control access to resources according to social connections associated with the resource host and that "[d]epending on the social connections associated with other users and/or devices associated with the other users as compared to the host user of the resources, the system **100** revokes or prevents access to the resources by the other users and/or the other devices."[13] It also states that "depending on one or more characteristics associated with the one or more resources, such as, for example, a number of users accessing the one or more resources, a traffic load associated with the one or more resources, or a combination thereof, the system **100** provokes or prevents access to the resources by other users and/or the other devices to maintain a quality of service provided by the one or more resources."[14] And then, with regard to the social networking information aspect of the solution, the specification goes on to explain that the system introduces the capability to determine whether the user and the host are a part of a particular social networking group and to control access to resources based on whether one is a part of such a shared social networking group. Additionally, other portions of columns 5 through 8 go on to reiterate these aspects of the proposed solutions to the above-referenced problems, or to provide more detailed possible implementations of such systems in order to control usage of wireless access points. So the point is that all those portions of

---

13 (*Id*., col. 4:53-61)

14 (*Id*., col. 4:61-5:1)

patent that I just described aren't simply speaking about "controlling access to resources" generally. They're clearly talking about *a particular way* to do so.

Claim 1 itself, unsurprisingly, includes lots of content about this particular solution. While the claim does start out by noting it[is] a method comprising the facilitating of the processing of data and/or information and/or at least one signal, and that it does so based in part on one or more resources (which can include one or more wireless access points) associated with at least one user or a combination thereof, the claim also explains that it does this in a particular way. That is, the claim notes[] that it does so by processing social networking information associated with the user or device or both to determine one or more social networking groups and by controlling access to the one or more resources vis-a-vis the user or device or both based, at least in part, on membership in one or more social networking groups and on certain characteristics associated with the resources, which must include "a number of users accessing the one or more wireless access points, a traffic load associated with the one or more wireless access points, or a combination thereof."[15] Put differently much of the claim is devoted not to claiming "controlling access to resources" generally. It[is] about the *more particular way* that the patent says it is going to go about doing this.

There[is] another reason why it doesn't make sense for the Court [to] conclude that claim 1 is directed simply to "controlling access to resources." The Court has noted that [a] prior art way of controlling access to wireless access points was to provide the same password to various potential users. That[is] surely a way of "controlling access to resources." But no one would say the patent is directed to *that* concept. After all, the patent disparages that concept repeatedly, and it takes pains to explain that the invention here is a *better solution than that* [to] the problem of controlling such access.

In light of all this, the Court does not agree with Defendant's argument that the claim is directed simply to the proposed abstract idea. It will thus recommend that the motion can be denied on that ground alone. Nevertheless, for sake of completeness, the Court will also now address the motion at step two. In other words, the Court will explain why, even assuming *arguendo* that it [is] wrong and claim 1 *is* directed to the abstract idea at issue, the claim should nevertheless survive the eligibility analysis at step [two].

---

[15] (*Id*., col. 26:10-14)

> At step two, if a claim is directed to an abstract idea, then the *Alice* framework requires the Court to assess "what else is there in the claims" by considering the "elements of each claim both individually and 'as an ordered combination'" in order to determine whether the "additional elements 'transform the nature of the claim' into a patent-eligible application."[16] The Supreme Court [of the United States] described step two in *Alice* as the search for an "inventive concept."[17]
>
> Although the Supreme Court used the term "inventive concept" to describe what it is that helps the patentee survive step two, the search for an inventive concept is not about whether the claimed element in question is new or unique.[18] Instead, an "inventive concept" is simply "an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself."[19]
>
> As was noted in *Amdocs (Israel) Limited [vs.] Openet Telecom, Inc.*,[20] a Federal Circuit case, and *Fitbit, Inc. [vs.] AliphCom*,[21] a case from the [United States District Court for the] Northern District of California, in the context of computer-focused claims, the addition of an element that simply requires a computer to work in its "conventional" manner (for example, to speed up the processing of an abstract idea) can't amount to an inventive concept. But the addition of elements that amount to the unconventional use of technology might be enough.

---

16 *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014) (certain internal quotation marks and citations omitted).

17 *Id.* (internal quotation marks and citations omitted).

18 *See Affinity Labs. of Tex., LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1263 n.3 (Fed. Cir. 2016).

19 *Alice*, 573 U.S. at 217-18 (certain internal quotation marks, brackets and citations omitted).

20 *Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1306 (Fed. Cir. 2016).

21 *Fitbit, Inc. v. AliphCom*, 233 F. Supp. 3d 799, 812-13 (N.D. Cal. 2017).

Here at step two, even if [] claim 1 [were said to be directed to the] abstract idea of "controlling access to resources," there would at least be a factual dispute, preventing grant of the motion, as to whether the "something more" in the claims—that is, the method's use of membership in a social networking group and its use of performance characteristics like traffic load and number of users to control access—amounts to an inventive concept.

In that regard, Plaintiff argues that claim 1 is a claim to a solution to a technical problem: "an improved authentication scheme that uses an association between the user[s] or their device and social networking group information and limits based on the number of user[s and] traffic loads."[22] As the Court has noted previously, there is support for this assertion in the record. The patent explains how, in the past, there were problems surrounding the giving of access to wireless access points, including those that cropped up via the use of a traditional password-based access system. The patent asserts that the claimed inventions and their utilization of social networking information and performance characteristics provide a better way to permit access to a wireless access point that solved that technological problem.

The Court notes that there[is] a dispute in the briefing, which was amplified during argument today, about whether claim 1's "controlling of access" step includes a requirement that the claim utilizes an "access control platform" in some way, and a dispute about what exactly that platform can do with social networking information, such as whether, for example, it can keep or maintain files on such information. But at best for [D]efendant, the question of whether the claim includes an access control platform and/or what is the extent of what that platform does would be a claim construction dispute not well-suited to be resolved today. At a minimum, it[is] clear the claimed method must process social networking information and control access to the resource based on that information, and that alone would be [sufficient] for the Court to find a relevant factual dispute at step two.

In other words, there[is] record support for the idea that the claimed solution can be said to provide *a more particularized way* of controlling access to resources that solves *a technological problem*. That[is] sufficient for the Court to recommend denial of the motion at step two.

---

[22] (D.I. 45 at 17)

Additionally, the Supreme Court in *Alice* noted that the concern that drives Section 101's exclusionary principle is "one of preemption[,]" driven by the concern that patent law not inhibit future discovery by improperly tying up the future use of building blocks and ingenuity.[23] In that regard, surely claim 1 does not preempt all ways of controlling access to resources, or anything close to that. The patent already tells us about one prior art way to do that that is not claimed: the use of manual passwords. And it would be hard to argue that there are no[t] myriad [] other ways to do so, other than by using membership in a social media group and reliance on certain limited types of performance characteristics.

The Court recognizes that the [D]efendant had a number of arguments in opposition to [the Court's] conclusion. I will address a few now.

Defendant, for example, argues that the claim does not sufficiently describe how it solves the problem of controlling access to wireless access points.[24] And here, the Court acknowledges that there is surely a level of "how" that claim 1 does not provide. More specifically, the claims don't, for example, specify *how* it is, from a technological perspective, that the method in question actually processes social networking information or *how* the method actually controls access to the resources (beyond the fact that it has to use a combination of characteristics described in the claims to do so). And it may well be that the specification also does not provide for much guidance in these regards either.

That said, as the Court noted previously, [the] claims do appear to make use[] of specific steps related to controlling access. This specificity, in the Court's view, is sufficient to survive step two.

Moreover, in *Visual Memory, LLC, v. NVIDIA Corp*., the Federal Circuit explained that "whether a patent specification teaches an ordinarily skilled artisan how to implement the claimed invention presents an enablement issue under 35 U.S.C. [§] 112, not an eligibility issue[] under [§] 101.["][25] Here, Defendant's concerns about lack of specificity sound more like the subject of a Section 112 challenge than a viable Section 101 argument.

---

23 *Alice*, 573 U.S. at 216.

24 (*See* D.I. 52 at 3-4)

25 *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253, 1261 (Fed. Cir. 2017).

The case law also supports the Court's decision in these regards.

> For example, in *CosmoKey Solutions GmbH [&] Co. KG v. Duo Sec[.] LLC*,[26] a Federal Circuit case cited by the [P]laintiff, the representative claim at issue disclosed a method for authenticating the identity of a user to a transaction at a computer. In other words, a method of preventing hacking. The Federal Circuit concluded at step two that the claim's limitations amounted to an inventive concept that was something more than the abstract idea at issue, which there was simply "authentication[.]"[27] The *CosmoKey* Court disagreed that the manner in which the claim performed authentication was "far from concrete."[28] Instead, the Court explained that "[h]ere, the claim limitations are more specific and recite an improved method for overcoming hacking by ensuring that the authentication function[] is normally inactive, activating only for a transaction, communicating the activation within a certain time window, and thereafter ensuring that the authentication function [i]s automatically deactivated."[29] In other words, as with the previously referenced aspects of claim 1 that are at issue here, these aspects of the *CosmoKey* claim provided a sufficient specificity to the method claim at issue there to ensure that the claim would not unduly monopolize the abstract idea at issue. This was so, even though the claim in *CosmoKey* never specified *how* the method transmitted a user identification or *how* it checked the identification function (beyond using the one criterion required by the claim) or *how* it ensured that the function was activated or inactivated at any step. Moreover, in *CosmoKey*, the Court was comforted in its conclusion that this solution was an inventive concept because the "specification explains that these features in combination with the other elements of the claim constitute an improvement that increase[s] computer and network security, prevents a third party from fraudulently identifying itself as the user, and is easy to implement and can be carried out even with mobile devices [of] low complexity."[30] Similarly here, the

---

[26] *CosmoKey Sols. GmbH & Co. KG v. Duo Sec. LLC*, 15 F.4th 1091 (Fed. Cir. 2021).

[27] *Id*. at 1095.

[28] *Id*. at 1099 (internal quotation marks and citation omitted).

[29] *Id*.

[30] *Id.*

specification of the '171 patent explains how the use of the social networking information and performance characteristics to control access to wireless access points also constitutes an improvement to technology that enabled devices like these to do things that they were not previously able to do.

Another helpful case for [P]laintiff is *SRI International, Inc. [vs.] Cisco Systems, Inc*.,[31] a Federal Circuit case that Plaintiff says is most similar to this one. In *SRI*, the representative claim was to a computer-automated method of hierarchical event monitoring and analysis within a network. The claim did so by deploying network monitors that detected suspicious activity based on an analysis of at least one of certain categories of network traffic data, then the monitors generated reports of suspicious activity, and then those reports were received and integrated. At step one, the *SRI* Court found that the claim was not simply directed to the abstract idea of "collect[ing] and analyz[ing] data."[32] Instead, the Court looked to the patent specification, which explained that the claimed invention solved weaknesses in conventional networks in order to fix a technical problem and provide a "framework for the recognition of more global threats to interdomain connectivity, including coordinated attempts to infiltrate or destroy connectivity across an entire network enterprise."[33] This was enough to assure the Court that the computers used in the claim were not added simply "as a tool" to automate conventional activity.[34] The *SRI* Court came to this conclusion even though the claim did not specify *how* the network monitors detected suspicious activity (beyond using at least one of the categories of data mentioned in the claim) or *how* they generated reports of suspicious activity or *how* they received and integrated those reports. As in *SRI*, here, there is a specific solution in the representative claim to the problem cited in the patent, and the patent tells us that this solution positively impacted others' ability to use wireless access network technology, even if the claim doesn't specify *every detail* of how access is controlled.

---

31 *SRI Int'l, Inc. v. Cisco Sys., Inc*., 930 F.3d 1295 (Fed. Cir. 2019).

32 *Id*. at 1304.

33 *Id*. at 1303-04 (internal quotation marks and citation omitted).

34 *Id*. at 1304.

In contrast, Defendant asserted that the *Ericsson* case from the Federal Circuit was the closest case to our facts, but in the Court's view, *Ericsson* is distinguishable. In *Ericsson*, the two representative claims were to a system for controlling access to a platform (or telecommunication system), and the Federal Circuit said that those claims were directed to the abstract idea of "controlling access to, or limiting permission to, resources."[35] The Court also concluded that there was no inventive concept found in the claims. The *Ericsson* Court explained that the claimed elements, essentially, were to an access controller that controlled access by receiving a request and then determining that the request should be granted. But the key in *Ericsson* was that the "claims are silent as to how access is controlled."[36] Indeed, the claims in *Ericsson* at issue never provided *any* meaningful level of detail, *any* real description of *how*[—]as to what specific factors were to be utilized in order to determine how access was granted. Instead, those claims, according to the *Ericsson* Court, "merely make generic functional recitations that requests are made and then granted."[37] Here, in contrast, claim 1 does provide some amount of specificity as to how requests for access should be granted, specifics that the patent tells us were unconventional if used in the claimed manner.

Defendant also argued that one of the key aspects of claim 1—using social networking group membership to control access to wireless access points—was not actually new at all. In support, Defendant[] cited to a portion of the prosecution history in which the [E]xaminer, in assessing a prior art reference known as Nath, appears to have concluded that Nath, in fact, disclosed this type of limitation. The Court understands Defendant to be making this argument because it believes that if it can show that the record conclusively establishes that this was not a new step, then this will blunt Plaintiff's argument that the limitations in claim 1 were, in fact, a new way of controlling access to wireless access points, and this will in turn harm Plaintiff's eligibility case.

The argument, however, doesn't alter the Court's decision. For one thing, there are other relevant limitations in the claim, such as the use of performance data to control access. The addition of such performance-data-related limitations appear to be what

---

35 955 F.3d at 1326.

36 *Id*. at 1328.

37 *Id.*

> caused the [E]xaminer to allow the patent to issue, along with the other aspects of the claim, and their existence in the claim could still help with Plaintiff's eligibility argument here. But the bigger point is that in citing to the prosecution history, all Defendant has done, at most, is to identify a factual dispute in the record: one about whether the use of social networking group membership to control access to wireless access points was novel. The [E]xaminer may have concluded that it was (and the [E]xaminer may have been right, or he may have been wrong to do so.)[.] But the patent, as I have noted, clearly asserts this was *not* conventional. And at the Rule 12(b)(6) stage, the Court must accept all of the Plaintiff's factual allegations as true and construe the record in the light most favorable to the [P]laintiff. Thus, from this record, I must infer that this use of social networking information was, in fact, a new way of attacking the network access[s] problem at issue. Nor do I think Defendant has demonstrated that as a legal or factual matter that Plaintiff somehow acquiesced to the [E]xaminer's conclusion about Nath, and Defendant has provided no caselaw suggesting that in circumstances like these, a plaintiff has been found to have so acquiesced. So this issue does not impact the Court's conclusion either.
>
> In sum, the Court recommends that Defendant's motion to dismiss on Section 101 grounds should be denied at step one with regard to the representative claim or, in the alternative, at step two. And as our Court has noted in cases like *F45 Training Party Limited v. Body Fit Training USA Inc.*,[38] and *eBuddy Techs. B.V. v. LinkedIn Corp.*,[39] since the motion should be denied as to Plaintiff's purportedly representative claim, it should also be denied as to all other asserted claims.

This Report and Recommendation is filed pursuant to 28 U.S.C. § 636(b)(1)(B), Fed. R. Civ. P. 72(b)(1), and D. Del. LR 72.1. The parties may serve and file specific written objections within fourteen (14) days after being served with a copy of this Report and Recommendation.

---

[38] *F45 Training Pty Ltd. v. Body Fit Training USA Inc.*, C.A. No. 20-1194-LPS, 2021 WL 2779130, at *5 (D. Del. July 2, 2021).

[39] *eBuddy Techs. B.V. v. LinkedIn Corp.*, Civil Action No. 20-1501-RGA-CJB, 2021 WL 7209517, at *10 (D. Del. Nov. 29, 2021), *report and recommendation adopted,* 2022 WL 733996 (D. Del. Mar. 11, 2022).

Fed. R. Civ. P. 72(b)(2). The failure of a party to object to legal conclusions may result in the loss of the right to *de novo* review in the district court. *See Sincavage v. Barnhart*, 171 F. App'x 924, 925 n.1 (3d Cir. 2006); *Henderson v. Carlson*, 812 F.2d 874, 878-79 (3d Cir. 1987).

The parties are directed to the Court's Standing Order for Objections Filed Under Fed. R. Civ. P. 72, dated March 7, 2022, a copy of which is available on the District Court's website, located at http://www.ded.uscourts.gov.

Christopher J. Burke
Christopher J. Burke
UNITED STATES MAGISTRATE JUDGE