IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

WSOU INVESTMENTS, LLC D/B/A BRAZOS LICENSING AND DEVELOPMENT,	)	C.A. No. 1:21-cv-1119-MN-CJB
Plaintiff,	)	**JURY TRIAL DEMANDED**
v.	)	
NETGEAR, INC.,	)	
Defendant.	)	

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff WSOU Investments, LLC d/b/a Brazos Licensing and Development ("Plaintiff"), through its attorneys, complains of Netgear, Inc. ("Defendant"), and alleges the following:

PARTIES

1. Plaintiff WSOU Investments, LLC d/b/a Brazos Licensing and Development is a limited liability company organized and existing under the laws of Delaware that maintains its principal place of business at 605 Austin Avenue, Suite 6, Waco, Texas 76701.

2. Defendant Netgear, Inc. is a corporation organized and existing under the laws of Delaware that maintains an established place of business at 350 E. Plumeria Drive, San Jose, California 95134.

JURISDICTION

3. This is an action for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code.

4. This Court has exclusive subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

5. This Court has personal jurisdiction over Defendant because it has engaged in systematic and continuous business activities in this District, and is incorporated in this District's state. As described below, Defendant has committed acts of patent infringement giving rise to this action within this District.

VENUE

6. Venue is proper in this District under 28 U.S.C. §§ 1391(b) and (c), and 28 U.S.C. § 1400(b) because Defendant has committed acts of patent infringement giving rise to this action in this District, has an established place of business in this District, and is incorporated in this District. In addition, Plaintiff has suffered harm in this District.

PATENT-IN-SUIT

7. Plaintiff is the assignee of all right, title and interest in United States Patent No. 9,338,171 ("the '171 Patent"), including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the '171 Patent. Accordingly, Plaintiff possesses the exclusive right and standing to prosecute the present action for infringement of the '171 Patent by Defendant.

THE '171 PATENT

8. The '171 Patent is entitled "Method and apparatus for controlling access to resources" and issued on May 10, 2016. The application leading to the '171 Patent was filed on December 19, 2012, and the provisional application was filed on December 30, 2011. A true and correct copy of the '171 Patent is attached hereto as **Exhibit 1** and incorporated herein by reference.

9. The '171 Patent is valid and enforceable.

The ’171 Patent Describes Technological Problems In Conventional Prior Art Networking Devices

10. Networking device manufacturers are continually challenged to deliver technological advancements over prior products in order to provide value and convenience to consumers. ’171 patent at 1:14-16. One such product is a system for sharing networking resources among various users. *Id*. at 1:16-17. By way of example, a user may wish to allow other users to access a networking resource, such as a wireless access point, when the designated users are within range of the access point. *Id*. at 1:17-21. Juxtaposed with the ability to enable users to share resources is the need to maintain security with respect to those resources, and to enable sharing of the resources without degradation of performance of the resources. *Id*. at 1:20-24. For example, a user that shares a wireless access point among designated users may wish to maintain a certain level of (i) security and (ii) performance of the wireless access point. *Id*. at 1:24-27.

11. While certain network resources may include security features, such security features were technologically limited. *Id*. at 1:28-30. For example, wireless access points were capable of being password protected. *Id*. at 4:14-17. The password protection is used to prevent unauthorized users from accessing the wireless access point without permission and eavesdropping on communications associated with other users connected to the access point. *Id*. at 4:17-23. Thus, although security associated with wireless access points is needed, it makes sharing wireless access points between family members, friends, and other users complex. *Id*. at 4:26-29.

12. For example, in prior art conventional networking devices, a password for accessing the access point must be generated and distributed among all of the users that are authorized to access the access point. *Id*. at 4:30-32. In other words, if a user walked into a coffee shop and wanted to connect a laptop or mobile phone to a wireless access point to use the Internet, then that user would need to request a username and password from the coffee shop owner and

then manually enter the username and password in order to be granted access. Conversely, for example, in order to revoke that user's permission to access an access point, the coffee shop owner would need to manually access the security settings for the access point to change the security settings (*e.g.*, password, revocation of a MAC address, etc.). *Id*. at 1:28-30. Even worse, to prevent a previously authorized user from accessing the access point, a new password must be created and distributed to each of the other authorized users, assuming they all shared the same password. *Id*. at 4:32-35. In fact, other even more complex processes may be necessary to prevent a previously authorized user from accessing the access point beyond merely changing the password. *Id*. at 4:35-38.

13. Further, beyond preventing unauthorized users from accessing an access point, prior art convention networking devices also suffered from problems associated with degradation of services based on, for example, the number of users associated with a wireless access point may exist. *Id*. at 4:38-42. Exacerbating these technical problems in prior art conventional networking devices are problems in controlling the wireless access points directly through, for example, the configuration settings associated with the access point. *Id*. at 4:42-45. For example, the configuration settings of the wireless access point must be accessible otherwise the settings cannot be changed. *Id*. at 4:45-47. Further, prior art conventional networking devices was limited to changing the settings only in a static way for controlling access to an access point and did not automatically update the user's credentials based on information or group memberships maintained in third-party networks. *Id*. at 4:47-50. Similar issues concern other types of resources, such as a database accessible over a network. *Id*. at 4:50-52. Thus, as of the date of the '171 patent, there was no system to control users' access to networking resources, such as wireless access points, through security an authentication mechanism using social networking information

associated with a user that could be independent of controlling the resource settings directly to maintain the security and performance of the resources.

The '171 Patent Teaches Specific Technological Solutions to the Problems Associated with Prior Art Conventional Networking Systems

14. To address the above-described technological problems in the prior art conventional networking systems, the inventors of the '171 patent created distributed networking systems and methods that include an access control platform for controlling access to a wireless access point based upon social connections and the performance of the wireless access point(s). *Id*. at 4:53-56. To that end, the inventors of the novel systems developed and included an access control platform that determines whether to grant a user access to a wireless access point based on that user's social networking group information. *See, e.g.*, *id*. at 7:26-30. More specifically, depending on the social connections associated with other users and/or other devices associated with the other users as compared, for example, to the host user of the resources, the system grants, revokes or prevents access to wireless access points. *Id*. at 4:56-61. The system also introduces the capability to control the security and performance of wireless access point independently from directly controlling the configuration of the resources by remotely controlling access to the wireless access point at the device level. *Id*. at 5:1-5, 5:50-6:2, 6:41-45, 13:45-14:8.

15. For example, the host of the novel wireless access point may remotely confirm the system to grant access to an entire membership of a Facebook group. The novel wireless access points' access control platform is capable of controlling the device's security and grant access to the entirety of the membership without manually creating and distributing individual credentials for each of the members. *See, e.g.*, *id*. at 5:6-32, 7:26-30, 8:5-42, Figs. 1-4, 6A-6D, 7. The novel system maintains, among other things, information (*e.g.*, profile information) about the members and their connection to the host, or requisite social networking groups. *See id*. The access control

platform utilizes the social networking information to authenticate a user that seeks to connect to the wireless access point. *See, e.g., id.* at 8:9-20. The authentication process may include determining the ability of the user's device to actually login based on the social networking information. *See, e.g., id.* In addition, the authentication process includes the novel wireless access point continuing to monitor the status of the membership list with respect to, for example, the host's social networking contacts or social networking platform groups. *See, e.g., id.* By monitoring the list of members of groups associated with the host or indicated as "friends" of the host, the access control platform is able to associate users and user devices with the wireless access point. *See, e.g., id.* at 8:16-20.

16. Additionally, the access control platform determines what access rights are made available to the one or more members of an associated group. *See, e.g., id.* at 8:21-23. Access rights may be based on, for example, whether a relationship identifier is family, friend, friend of a friend, acquaintance, other, etc. *See, e.g., id.* at 8:23-25. In other instances, the indicator may relate to some other level of closeness, familiarity or priority of the host relative to the member. *See, e.g., id.* at 8:25-28. In that same vein, the novel wireless access point includes a configuration to set a hierarchy of priority for access by different groups depending upon social networking information. *See, e.g., id.* at 6:49-56. For example, if a user that is classified within the social networking group of family is currently accessing the wireless access point, if another user that is classified within the social networking group of friends attempt to access the same access point, the latter may be prevented from accessing the resource based on the former user having a higher priority. *See, e.g., id.* at 6:56-63. Similarly, if the friend user has access to the wireless access point and a family user attempts to access the same access point, the friend user may have their access revoked to ensure security of the family user using the wireless access point. *See, e.g., id.*

at 6:63-66. Accordingly, lower-priority users, and devices associated with lower-priority users, have their access to the wireless access point revoked or barred based on access to the same by higher-priority users based on the social networking groups. *See, e.g., id.* at 6:66-7:3. By controlling the revocation and prevention of access to the wireless access point based on the priority hierarchy of users or their devices, hosts that maintain the wireless access point may open them to a wider range of users while maintaining a level of security for more trusted users or users that have a closer social relationship to the host. *See, e.g., id.* at 16:4-10.

17. Further, the access control platform includes an additional security feature for preventing a malicious or unauthorized user from tampering with the novel wireless access point. *See, e.g., id.* at 8:43-47, 12:27-59. Such a malicious user may obtain the security credentials for accessing the wireless access point and disable the credentials effectively enabling the malicious user to use wireless access point even if not intended by the host of the resources. *See, e.g., id.* at 8:48-52, 12:27-59. To implement additional security, the access control platform monitors for the user and user's device that attempts to access the wireless access point to ensure that user or user's device are accessing the wireless access point according to the established hierarchies and/or the characteristics of the wireless access point. *See, e.g., id.* at 8:52-56, 12:27-59. For example, the access control platform will monitor for the user and user device accessing an access point and determine whether the user has actual authority to access the access point according to the hierarchy as compared to other user devices currently accessing the access point. *See, e.g., id.* at 8:56-61, 12:27-59. If the access control platform determines that unauthorized user device is accessing the wireless access point, the access control platform may act to eliminate access rights by the malicious user or device to the wireless access point. *See, e.g., id.* at 8:61-56, 12:27-59.

18. Moreover, the access control platform also controls access to the wireless access point based on either or both of (i) the number of users accessing the wireless access point and (ii) the traffic load of the wireless access point(s), which may be the bandwidth of the same. *See, e.g.*, *id*. at 4:61-5:5, 7:4-25, 16:11-32, Figs. 4, 5. For example, the access control platform will not grant or will prevent a user's access to a wireless access point if that the inclusion of an additional user exceeds the limit users for the access point. *See, e.g.*, *id*. at 16:11-32, Figs. 4, 5. These limitations are to ensure that the performance of the wireless access points remains and do not degrade. *See, e.g.*, *id*. at 4:61-5:5, 5:33-37, 7:4-25, 16:11-32.

19. As an example, the owner of Joe's Coffee Shop is the creator of a Facebook group named "Joe's Coffee Shop," which includes 1,000 members. The owner seeks to permit all 1,000 members of that Facebook group with access to a wireless access point in Joe's Coffee Shop without having to create 1,000 different user names and passwords in order to grant access to the Internet when any of the group's members patronize the coffee shop. The owner could remotely set the novel wireless access point in the coffee shop to provide access to the entire membership of the Facebook group Joe's Coffee Shop. *See, e.g.*, *id*. at 7:65-8:7. The wireless access point is capable of associating the membership of the Facebook group with their respective devices. If a member of the group walks into Joe's Coffee Shop and the member's mobile phone is located within the range of the wireless access point, the access control platform utilizes that social networking information (*e.g.*, Joe's Coffee Shop group membership) to authenticate the member's credentials and grant access to the wireless access point. *See, e.g.*, *id*. at 7:65-8:8-34. Alternatively, the member could also input its Facebook username and password to be authenticated by the access control platform, which would be in lieu of a separate and distinct username and password supported only for the wireless access point. However, before the novel

wireless access point grants access to the group member, it would need to ensure that the addition of the member would not exceed the user limit or negatively impact the traffic load of the access point.

20. Thus, the '171 patent claims and specification recite specific technological improvements to prior art convention wireless access points where control of a user's access is based on a security authentication mechanism using social networking information and resource performance to prevent unauthorized access that is remotely and efficiently implemented and can advantageously be carried out with mobile devices of low complexity.

21. Alternatively, each of the above-described technical improvements, either separately or taken together, are considered "additional elements" that are taken a non-generic, non-conventional ordered combination that further "transform" the claimed system "into a patent eligible" invention. Moreover, the '171 patent teaches a distributed architecture, where the claimed wireless access point can receive automatic updates of a user's membership in the requisite social networking groups from third-party social networking platforms as a basis to authenticate users' devices to grant them access to the wireless access point. The incorporation of this improvement over the prior art conventional networking systems is part of the non-generic, non-conventional ordered combination of elements that provide an inventive concept that transforms the claimed system into a patent eligible invention.

COUNT 1: INFRINGEMENT OF THE '171 PATENT

22. Plaintiff incorporates the above paragraphs herein by reference.

23. **Direct Infringement.** Defendant has been and continues to directly infringe one or more claims of the '171 Patent in at least this District by making, using, offering to sell, selling and/or importing, without limitation, at least the Defendant product identified in the chart

incorporated into this Count below ("Exemplary Defendant Product") that infringes at least claim 1 of the '171 Patent also identified in the chart incorporated into this Count below (the "Exemplary '171 Patent Claim") literally or by the doctrine of equivalents. On information and belief, numerous other devices that infringe the claims of the '171 Patent have been made, used, sold, imported, and offered for sale by Defendant and/or its customers.

24. Defendant also has and continues to directly infringe, literally or under the doctrine of equivalents, the Exemplary '171 Patent Claim, by having its employees internally test and use the Exemplary Product.

25. **Actual Knowledge of Infringement.** Plaintiff has had actual knowledge of the '171 Patent since at least the service of Plaintiff's Complaint in the United States District Court for the Western District of Texas on February 23, 2021, in Case No. 6:21-cv-00154-ADA ("February 2021 Complaint"), which attached claim charts and corresponding reference exhibits comparing the Exemplary '171 Patent Claim to the Exemplary Product; these charts undoubtedly informed Defendant as to how the Exemplary Product infringes the '171 Patent.

26. Despite such actual knowledge, Defendant continues to make, use, test, sell, offer for sale, market, and/or import into the United States, products that infringe the '171 Patent. On information and belief, Defendant has also continued to sell the Exemplary Defendant Product and distribute product literature and website materials inducing end users and others to use its products in the customary and intended manner that infringes the '171 Patent. *See* Exhibit 2 (extensively referencing these materials to demonstrate how they direct end users to commit patent infringement). By the time of trial, Defendant will have known and intended (since receiving actual notice on February 23, 2021) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the '171 Patent.

27. Consequently, Defendant's infringement of the '171 Patent is willful and deliberate, entitling Plaintiff to enhanced damages pursuant to 35 U.S.C. § 284.

28. **Induced Infringement.** At least since being served with the February 2021 Complaint and corresponding claim charts, Defendant has committed, and continues to commit, affirmative acts that cause infringement, literally and/or by the doctrine of equivalents, of one or more claims of the '171 Patent with knowledge of the '171 Patent and knowledge that the induced acts constitute infringement of one or more claims of the '171 Patent. Defendant has actively induced others, including, but not limited to, customers, purchasers, developers, and/or end users of the Exemplary Defendant Product to infringe the '171 Patent, literally and/or by the doctrine of equivalents, throughout the United States, including within this judicial district, by, among other things, advertising, promoting, and instructing the use of the Exemplary Defendant Product via various websites, including providing and disseminating product descriptions, operating manuals, how-to videos and guides, and other instructions on how to implement and configure the Exemplary Defendant Product. Defendant induces others to infringe the '171 Patent by encouraging and facilitating others to perform actions that Defendant knows to be acts of infringement of the '171 Patent with intent that those performing the acts infringe the '171 Patent.

29. As an illustrative example only, Defendant induces such acts of infringement by its affirmative actions of intentionally providing the Exemplary Defendant Product that when used in their normal and customer way as desired and intended by Defendant, infringe one or more claims of the '171 Patent and/or by directly or indirectly providing instructions on how to use its Exemplary Defendant Product in a manner or configuration that infringes one or more claims of the '171 Patent, including at least the following:

- https://www.downloads.netgear.com/files/GDC/WAC505/WAC505_UM_EN.pdf

30. Defendant therefore actively, knowingly, and intentionally has been and continues to induce infringement of the ’171 Patent, literally or by the doctrine of equivalents, by instructing, encouraging or aiding others (including its customers, purchasers, developers, and/or end users) to make, use, sell, or offer to sell the Exemplary Defendant Product and other infringing products in the United States, or to import them into the United States, without license or authority from Plaintiff with knowledge of or willful blindness to the fact that Defendant’s actions will induce others, including but not limited to its customers, partners, and/or end users to infringe the ’171 Patent. Defendant induces others to infringe the ’171 Patent by encouraging and facilitating others to perform actions that Defendant knows to be acts of infringement of the ’171 Patent with intent that those performing the acts infringe the ’171 Patent.

31. **Contributory Infringement.** At least since being served with the February 2021 Complaint and corresponding claim charts, Defendant has committed, and continues to commit, contributory infringement, literally and/or by the doctrine of equivalents, by, *inter alia*, knowingly selling the Exemplary Defendant Product that when used causes the direct infringement of one or more claims of the ’171 Patent by a third party, and which has no substantial non-infringing uses, or include a separate and distinct component that is especially made or especially adapted for use in infringement of the ’171 Patent, and is not a staple article or commodity of commerce suitable for substantial non-infringing use.

32. Defendant therefore actively, knowingly, and intentionally has been and continues to materially contribute to its own customers’, purchasers’, developers’, and end users’ infringement of the ’171 Patent, literally or by the doctrine of equivalents, by selling Exemplary Defendant Product and other infringing products to their customers for use in end-user products in a manner that infringes one or more claims of the ’171 Patent. The Exemplary Defendant Product

and other infringing products are especially made or adapted for infringing the '171 Patent and are not staple articles of commerce suitable for substantial non-infringing uses. For example, in view of the preceding paragraphs, the Exemplary Defendant Product contains functionality which is material to at least one claim of the '171 Patent. *See* Exhibit 2 (demonstrating how end-user use of the Exemplary Defendant Product inevitably leads to infringement).

33. **Exhibit 2** includes a chart comparing the Exemplary '171 Patent Claim to the Exemplary Defendant Product. As set forth in the chart, the Exemplary Defendant Product practices the technology claimed by the '171 Patent. Accordingly, the Exemplary Defendant Product incorporated in the chart satisfies all elements of the Exemplary '171 Patent Claim.

34. Plaintiff therefore incorporates by reference in its allegations herein the claim chart of Exhibit 2, and corresponding referenced exhibits.

35. Plaintiff has been damaged by Defendant's infringement of the '171 Patent and will continue to be damaged by such infringement. Plaintiff is entitled to recover damages from Defendant adequate to compensate it for Defendant's infringement, in an amount measured by no less than a reasonable royalty under 35 U.S.C. § 284, as well as enhanced damages pursuant to 35 U.S.C. § 284.

JURY DEMAND

36. Under Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff respectfully requests a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

A. A judgment that the '171 Patent is valid and enforceable;

B. A judgment that Defendant has infringed directly, contributorily, and/or induced infringement of one or more claims of the ’171 Patent;

C. An accounting of all damages not presented at trial;

D. A judgment that awards Plaintiff all appropriate damages under 35 U.S.C. § 284 for Defendant’s past infringement with respect to the ’171 Patent;

E. A judgment that awards Plaintiff all appropriate damages under 35 U.S.C. § 284 for Defendant’s continuing or future infringement, up until the date such judgment is entered with respect to the ’171 Patent, including pre- and post-judgment interest, costs, and disbursements as justified under 35 U.S.C. § 284;

F. A judgment that awards Plaintiff ongoing royalties for Defendant’s continued direct and/or indirect infringement of the ’171 Patent;

G. A judgment awarding Plaintiff enhanced damages pursuant to 35 U.S.C. § 284, including for Defendant’s willful infringement of the ’171 Patent;

H. And, if necessary, to adequately compensate Plaintiff for Defendant’s infringement, an accounting:

i. that this case be declared exceptional within the meaning of 35 U.S.C. § 285 and that Plaintiff be awarded its reasonable attorneys’ fees against Defendant that it incurs in prosecuting this action;

ii. that Plaintiff be awarded costs, and expenses that it incurs in prosecuting this action; and

iii. that Plaintiff be awarded such further relief at law or in equity as the Court deems just and proper.

Dated: November 9, 2021

Respectfully submitted,

OF COUNSEL:

Jonathan K. Waldrop
Darcy L. Jones
Marcus A. Barber
ThucMinh Nguyen
John W. Downing
Heather S. Kim
Jack Shaw
KASOWITZ BENSON TORRES LLP
333 Twin Dolphin Drive, Suite 200
Redwood Shores, CA 94065
(650) 453-5170
jwaldrop@kasowitz.com
djones@kasowitz.com
mbarber@kasowitz.com
tnguyen@kasowitz.com
jdowning@kasowitz.com
hkim@kasowitz.com
jshaw@kasowitz.com

Shelley Ivan
KASOWITZ BENSON TORRES LLP
1633 Broadway
New York, NY 10019
(212) 506-1700
sivan@kasowitz.com

Paul G. Williams
KASOWITZ BENSON TORRES LLP
1230 Peachtree Street, NE, Suite 2445
Atlanta, GA 30309
(404) 260-6080
pwilliams@kasowitz.com

DEVLIN LAW FIRM LLC

By: */s/ James M. Lennon*
James M. Lennon (No. 4570)
1526 Gilpin Avenue
Wilmington, DE 19806
(302) 449-9010
jlennon@devlinlawfirm.com

Attorneys for Plaintiff
WSOU Investments LLC d/b/a
Brazos Licensing and Development