IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

BACKERTOP LICENSING LLC, **Plaintiff,** **v.** **BLACKBERRY CORP.,** **Defendant.**	**CIVIL ACTION NO.: 6:22-cv-1013** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

1. This is an action under the patent laws of the United States, Title 35 of the United States Code, for patent infringement in which Backertop Licensing LLC ("Backertop" or "Plaintiff") makes the following allegations against Blackberry Corporation ("Blackberry" or "Defendant").

PARTIES

2. Plaintiff is a Texas limited liability company, having its primary office at 2100 14th St., Suite 107 (PMB 1044), Plano, TX 75074 located in Collin County, Texas – within the Eastern District of Texas.

3. Defendant is registered as a domestic corporation in the state of Delaware, and has a principal place of business at Suite 400, 3001 Bishop Drive, San Ramon, CA 94583. Defendant also has a regular and established place of business at Suite 410, Domain Seven, 11501 Alterra Parkway, Austin, TX 78758. Defendant's Registered Agent for service of process in Texas appears to be Corporate Creations Network Inc., 5444 Westheimer, Suite #1000, Houston, TX 77056.

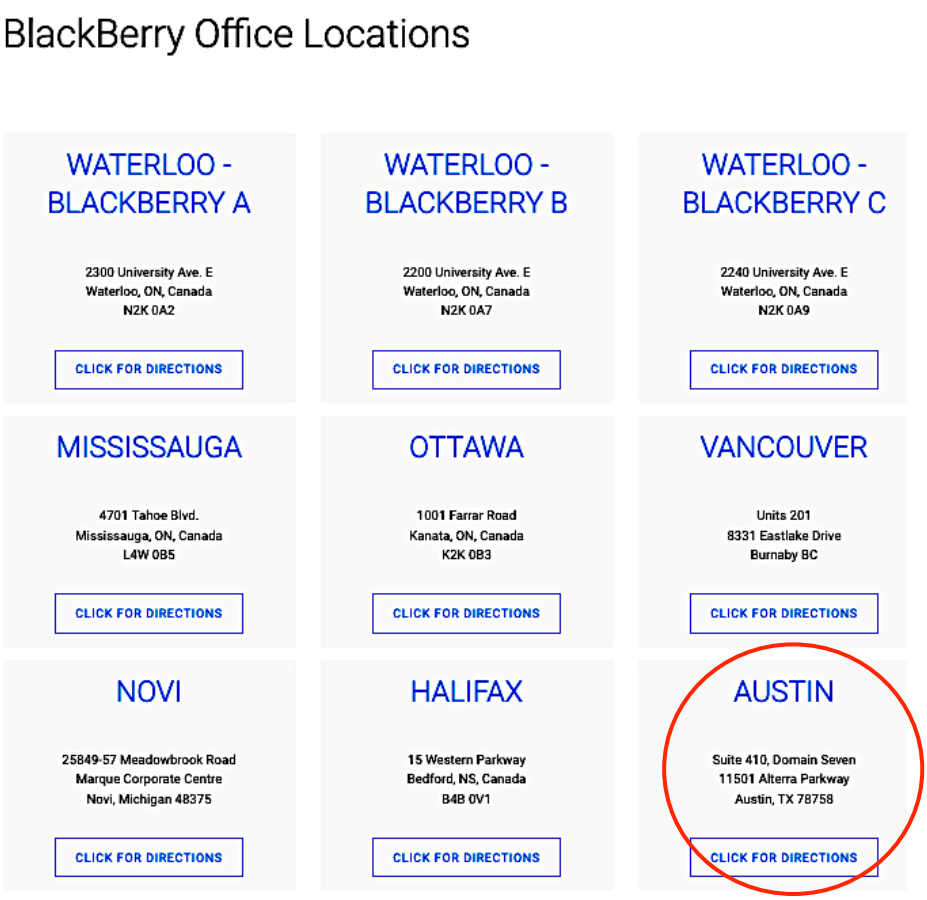
JURISDICTION AND VENUE

4. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. Venue is proper in this district under 28 U.S.C. §§ 1391(c), generally, and under 1400(b), specifically. Defendants have a regular and established place of business in this Judicial District, and Defendants have also committed acts of patent infringement in this Judicial District.

6. Defendants are subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to their substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

7. Defendant's website lists its office locations, including its office in Austin, TX:



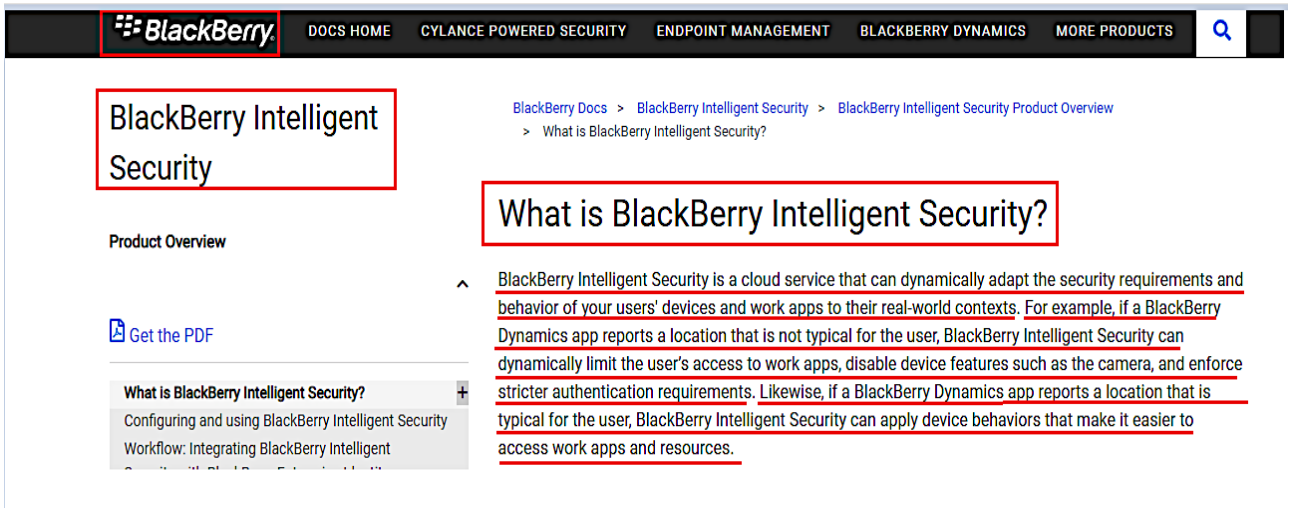
8. Defendant has infringed, and does infringe, by operating, transacting, and conducting business within the Western District of Texas.

9. Defendant's office in Austin, TX is a regular and established place of business in this Judicial District, and Defendant has committed acts of infringement within this District. Venue is therefore proper in this District under 28 U.S.C. § 1400(b).

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 9,332,385

10. Plaintiff is the owner by assignment of the valid and enforceable United States Patent No. 9,332,385 ("the '385 Patent") entitled "Selectively Providing Content to Users Located Within a Virtual Perimeter" – including all rights to recover for past, present and future acts of infringement. The '385 Patent issued on May 3, 2016, and has a priority date of February 13, 2015. A true and correct copy of the '385 Patent is attached as Exhibit A.

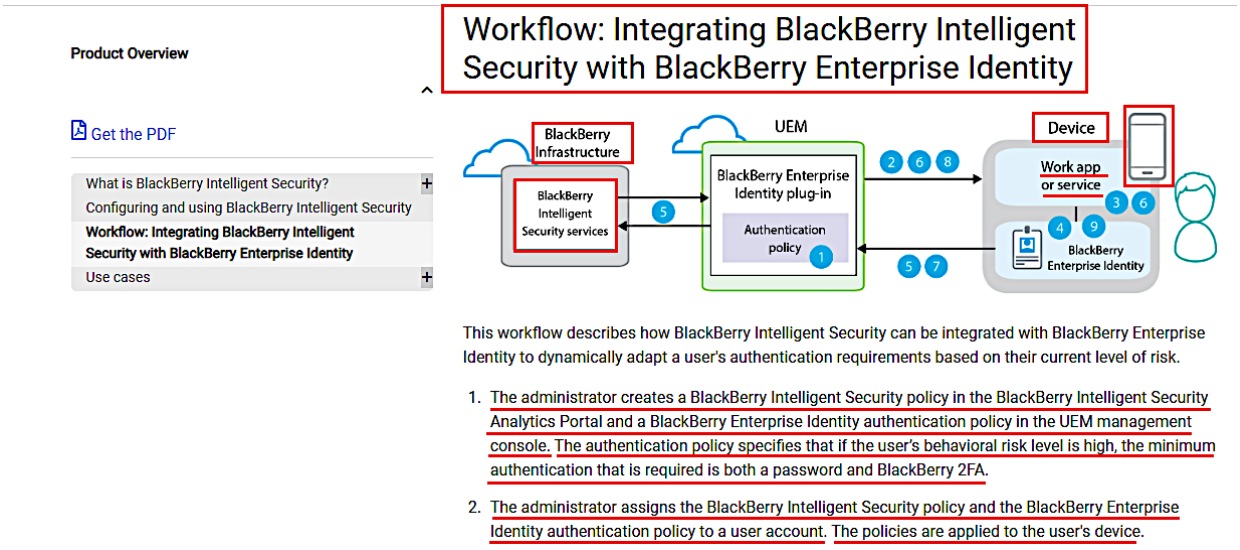
11. Defendant produces, sells, and offers for sale, cloud based security platforms and services – including, but not limited to, Defendant's Blackberry Intelligent Security System software and services ("Blackberry Systems").



12. More specifically, the Blackberry Systems that Defendant directly makes, uses, sells and offers for sale, are the infringing instrumentalities ("Defendant's Infringing Instrumentalities" or "Infringing Instrumentalities").

13. The Defendant's Infringing Instrumentalities operate based upon wireless communication between a mobile device (*e.g.*, user's work mobile device) and at least one

beacon (*e.g.*, Blackberry Unified Endpoint Management ("UEM") system connected via WiFi), to identify the location of the mobile device:



Jane Smith arrives at the airport for a business trip. She uses her work device, an iPhone, to access the airport's free Wi-Fi network.

The BlackBerry Dynamics apps on Jane's iPhone send data to the BlackBerry Intelligent Security services indicating that she is on a less secure network and that she is in a location that is far away from her typical learned location for that day and time. The services calculate a high behavioral risk level and a high geozone risk level and communicate these assessments to Jane's work apps, the BlackBerry Intelligent Security Analytics Portal, and UEM. The BlackBerry Intelligent Security policy that is applied to Jane's device takes effect, assigning Jane to a group with more restrictive device policies and profiles to ensure a higher level of security while Jane is at the airport.

14. The infringing instrumentalities utilize a Blackberry Dynamics App installed on the user's work mobile device to retrieve location data. The Blackberry dynamics app identifies the current physical location of the user mobile device using Wi-Fi network and reports it to Blackberry Intelligent Security System.

Jane Smith arrives at the airport for a business trip. She uses her work device, an iPhone, to access the airport's free Wi-Fi network.

The BlackBerry Dynamics apps on Jane's iPhone send data to the BlackBerry Intelligent Security services indicating that she is on a less secure network and that she is in a location that is far away from her typical learned location for that day and time. The services calculate a high behavioral risk level and a high geozone risk level and communicate these assessments to Jane's work apps, the BlackBerry Intelligent Security Analytics Portal, and UEM. The BlackBerry Intelligent Security policy that is applied to Jane's device takes effect, assigning Jane to a group with more restrictive device policies and profiles to ensure a higher level of security while Jane is at the airport.

15. Defendant's Infringing Instrumentalities operate using memory on the mobile device by storing the program code for the Infringing Instrumentalities in that memory. That program code is then executed by a processor associated with the mobile device to operate as described herein.

16. The Defendant's Infringing Instrumentalities identify a present physical location of such a mobile device:

The BlackBerry Intelligent Security services gather and process behavioral data, app events, and location data to calculate risk levels for each user in real-time:

- Behavioral risk: An assessment of risk (low, medium, or high) based on the user's typical activities.
- Continuous authentication risk: An assessment of risk based on a model of the user's typical usage of a BlackBerry Dynamics app. If the app reports behaviors or events that do not fit the user's model, BlackBerry Intelligent Security triggers an authentication prompt and the user must prove their identity if they want to continue using the app. Continuous authentication is currently supported only for BlackBerry Work.
- Geozone risk: An assessment of risk (low, medium, or high) based on the user's proximity to learned locations. You can also define custom geozones with static risk levels (for example, a specific office location with a low risk level).

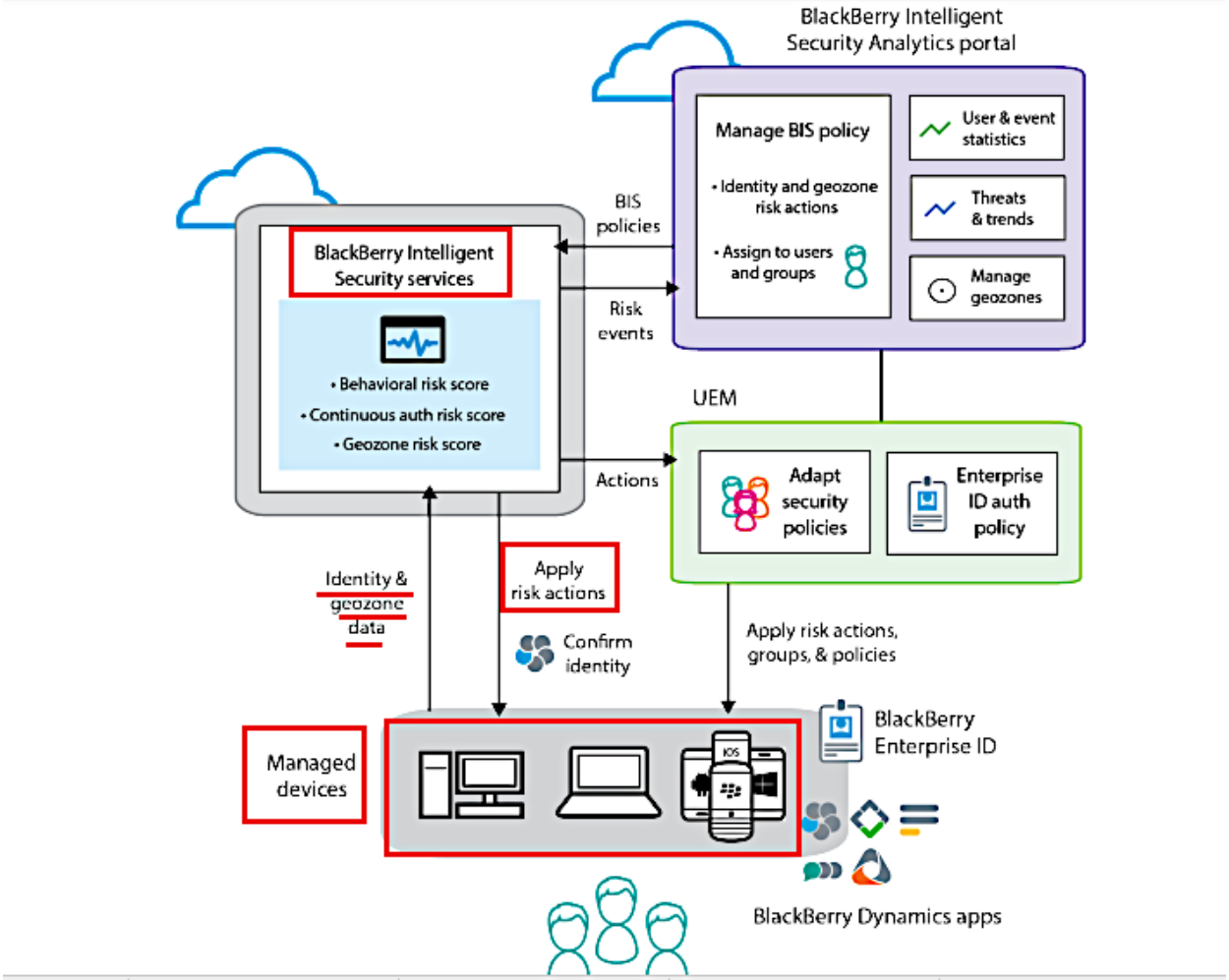
Jane Smith arrives at the airport for a business trip. She uses her work device, an iPhone, to access the airport's free Wi-Fi network.

The BlackBerry Dynamics apps on Jane's iPhone send data to the BlackBerry Intelligent Security services indicating that she is on a less secure network and that she is in a location that is far away from her typical learned location for that day and time. The services calculate a high behavioral risk level and a high geozone risk level and communicate these assessments to Jane's work apps, the BlackBerry Intelligent Security Analytics Portal, and UEM. The BlackBerry Intelligent Security policy that is applied to Jane's device takes effect, assigning Jane to a group with more restrictive device policies and profiles to ensure a higher level of security while Jane is at the airport.

17. The Defendant's infringing instrumentalities allow an administrator to create various policies, to be assigned to the user based on user's current geozone risk level. The accused instrumentality practices defining geozone with high, medium, or low risk level. For a typical learned geozone or a defined geozone such as a specific office location, the user geozone risk level is low.

The BlackBerry Intelligent Security services gather and process behavioral data, app events, and location data to calculate risk levels for each user in real-time:

- Behavioral risk: An assessment of risk (low, medium, or high) based on the user's typical activities.
- Continuous authentication risk: An assessment of risk based on a model of the user's typical usage of a BlackBerry Dynamics app. If the app reports behaviors or events that do not fit the user's model, BlackBerry Intelligent Security triggers an authentication prompt and the user must prove their identity if they want to continue using the app. Continuous authentication is currently supported only for BlackBerry Work.
- Geozone risk: An assessment of risk (low, medium, or high) based on the user's proximity to learned locations. You can also define custom geozones with static risk levels (for example, a specific office location with a low risk level).



BlackBerry Dynamics apps send app events and location data to the BlackBerry Intelligent Security services at regular intervals. BlackBerry Enterprise Identity sends data to the services at runtime. The services processes this data to generate identity and geozone risk scores in real-time for each user. Based on your configuration of the policy, BlackBerry Intelligent Security executes management actions that correspond to a user's risk level (for example, assigning the user to a UEM group or temporarily blocking BlackBerry Dynamics apps).

Based on your configuration of the BlackBerry Enterprise Identity authentication policy, a user's current behavioral risk level, geozone risk level, or a defined geozone can also determine how the user logs in to services and work apps (for example, no authentication, single sign-on, password, BlackBerry 2FA, or a combination of methods).

18. When the Blackberry Dynamics app sends location data to Blackberry Intelligent Security System, it determines geozone level based on the received current location of the user.

The BlackBerry Intelligent Security services gather and process behavioral data, app events, and location data to calculate risk levels for each user in real-time:

- Behavioral risk: An assessment of risk (low, medium, or high) based on the user's typical activities.
- Continuous authentication risk: An assessment of risk based on a model of the user's typical usage of a BlackBerry Dynamics app. If the app reports behaviors or events that do not fit the user's model, BlackBerry Intelligent Security triggers an authentication prompt and the user must prove their identity if they want to continue using the app. Continuous authentication is currently supported only for BlackBerry Work.
- Geozone risk: An assessment of risk (low, medium, or high) based on the user's proximity to learned locations. You can also define custom geozones with static risk levels (for example, a specific office location with a low risk level).

19. The infringing instrumentalities communicate an assigned policy (*i.e.*, a first message) to work apps and other applications associated with, and configured for the detected risk location of, the user's work mobile device.

Define geozones

When you define a geozone, you assign it a risk level to it (low, medium, or high). When you configure a BlackBerry Intelligent Security policy, you can add a defined geozone that will take precedence over the regular geozone risk actions in the policy (see Create a BlackBerry Intelligent Security policy). For example, you can define a geozone for a specific office location with a low risk level. If a user is in that geozone, their risk level will be low regardless of how far it is from their learned geozones. Note that the overall assessment of the user's geozone risk level is also impacted by the user's current behavioral risk assessment.

You can choose whether you want BlackBerry Intelligent Security to use learned geozones when it determines a user's geozone risk level. For example, you can disable learned geozones and configure the service to take action based on whether the user is in one of several defined geozones. You can set a default action for users that are not in a defined geozone.

How does BlackBerry Intelligent Security determine a user's geozone risk level?

The BlackBerry Intelligent Security services process event and location data from apps to learn about the locations (geozones) that are typical for each user at different times. You can configure a BlackBerry Intelligent Security policy to execute risk actions based on the user's proximity to a learned geozone.

For example, if a user is in the range of a learned geozone at a given day and time, their geozone risk level is low and the assigned policy executes the actions for the low risk level. Likewise, if the user is out of the range of a learned geozone, their geozone risk level is medium or high (depending on how far out of range the user is) and the assigned policy executes the corresponding actions. You can customize the range for each geozone risk level.

The services can learn new geozones for a user over time. The first time a user occupies a new location that is outside of their typical geozones, their behavioral and geozone risk levels may be higher than usual, but if the user is reported at that location with greater frequency, it can become a new learned geozone that results in a lower risk level.

20. As they determine that the current mobile device location is a high-risk zone, the infringing instrumentalities communicate with, for example, work apps on the mobile device to restrict their direct access, and to temporarily disable other apps such as camera, Bluetooth, etc., according to the assigned policy for the identified current location of the user's work mobile device.

Create a BlackBerry Intelligent Security policy

You configure a BlackBerry Intelligent Security policy to determine which groups UEM will automatically assign to a user based on the user's current behavioral risk level and geozone risk level.

You can select a different UEM group for each risk level, the same group for multiple risk levels, or you can choose to not take any action for a risk level. For more information about how UEM resolves any conflicting policy, profile, role, or app assignments, see Resolving conflicting assignments and precedence rules.

You can customize the policy to suit your organization's needs. For example, you can choose to take actions for geozone risk levels only and disable actions for behavioral risk levels, or you can disable learned geozones and configure actions based on whether the user currently occupies a defined geozone (for example, an office location that you have specified).

When the new group configuration is applied to Jane's iPhone, she notices the following changes:

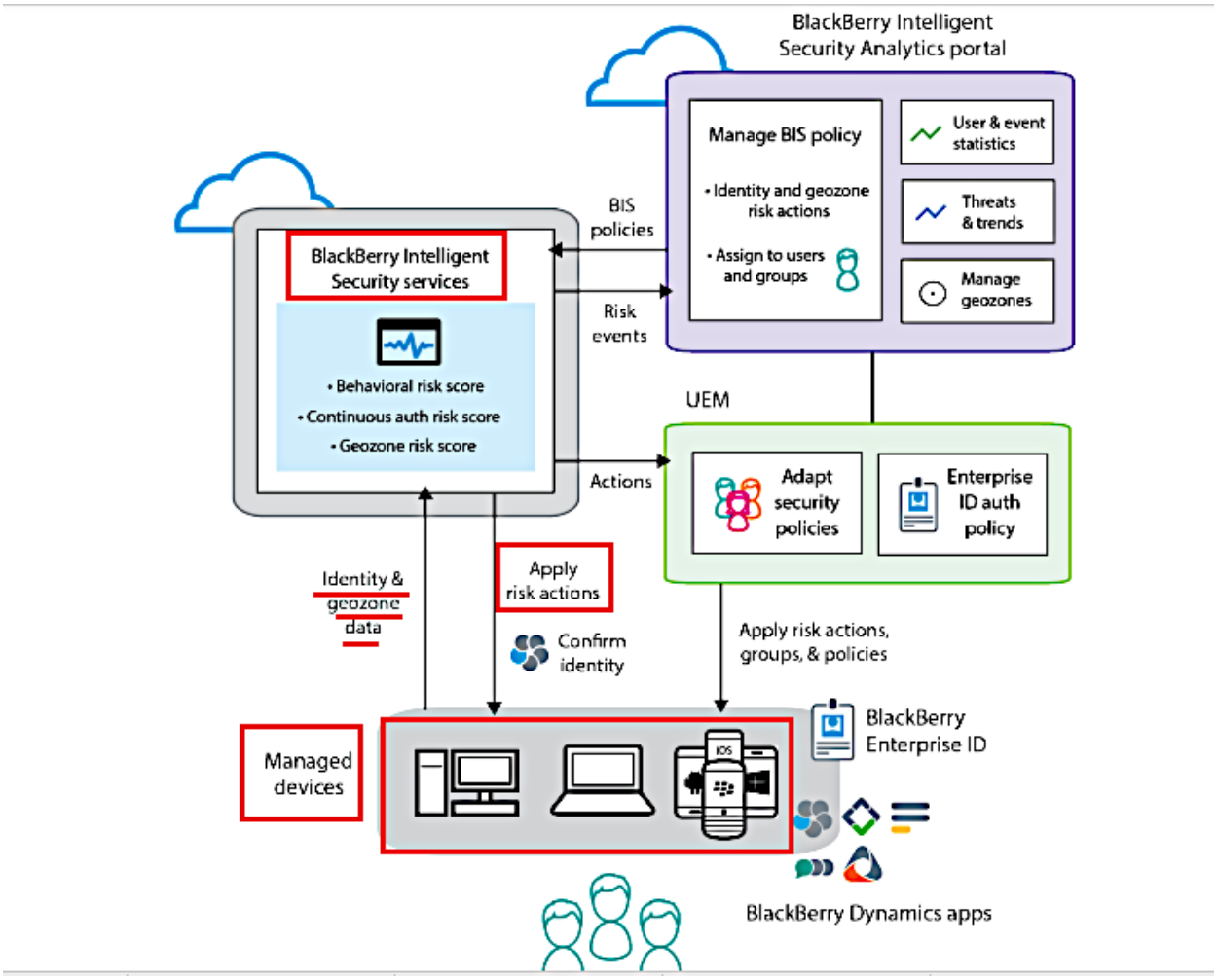
- When she tries to log in to work apps and services, she must provide both a UEM password and complete BlackBerry 2FA authentication.
- The iPhone camera is temporarily disabled.
- Bluetooth functionality is temporarily disabled.
- Her access to the company's intranet websites is currently restricted.
- Data synchronization to work apps, such as BlackBerry Work, occurs less frequently.

The new group assignment with these high-security device behaviors remains in place until Jane's behavioral and geozone risk level is recalculated and reduced. When she has a lower risk level, BlackBerry Intelligent Security will reassign her to a group that corresponds to the new risk level.

You can choose which risk engines you want BlackBerry Intelligent Security to use. For the different types and levels of risk, you can configure actions that you want BlackBerry Intelligent Security to execute when a user meets that risk criteria, including:

- Assigning the user to a local UEM group with policies, profiles, apps, and permissions appropriate for that risk level
- Temporarily blocking all BlackBerry Dynamics apps
- Temporarily blocking the specific BlackBerry Dynamics app that initiated the risk assessment

22. The infringing instrumentalities apply different policies according to a user device's location. A policy maintains the presence of the user device on a network (*e.g.*, Wi-Fi) at the current location of the user device.



Device Type	Name	Description	Activation types
iOS	Allow Files app to use USB (supervised only)	Specify whether the Files app can access files using a USB connection.	MDM controls
iOS	Allow Files app to connect to network drives (supervised only)	Specify whether the Files app can access files stored on a network drive.	MDM controls
iOS	Force Wi-Fi to be enabled (supervised only)	Specify whether Wi-Fi is always enabled on the device. If this rule is selected, users can't turn Wi-Fi off using the Device Settings or Control Center and Airplane Mode doesn't disable Wi-Fi.	MDM controls

23. Plaintiff herein restates and incorporates by reference paragraphs 11 – 22, above.

24. All recited elements of – at least – claims 1 and 8 of the '385 Patent are present within the structure and/or operation of Defendant's infringing instrumentalities.

25. Defendant's infringing instrumentalities comprise systems that identify a present physical location of a mobile device, based upon wireless communication between the mobile device and at least one beacon.

26. Defendant's infringing instrumentalities determine that the mobile device is located at a particular physical location.

27. Defendant's infringing instrumentalities communicate at least a first message to the mobile device, responsive to determining that the mobile device is located at the particular physical location.

28. Defendant's infringing instrumentalities communicate at least a first message to the mobile device that specifies at least one application to be disabled while the mobile device is present at the physical location.

29. Defendant's infringing instrumentalities receive a response to the first message from the mobile device, indicating that the at least one application is disabled.

30. Defendant's infringing instrumentalities authorize, using a processor, the mobile device to establish presence on a network maintained for the physical location, responsive to the response to the first message.

31. Defendant's infringing instrumentalities infringe – at least – claims 1 and 8 of the '385 Patent.

32. Defendant's infringing instrumentalities literally and directly infringe – at least – claims 1 and 8 of the '385 Patent.

33. Defendant's infringing instrumentalities perform or comprise all required elements of – at least – claims 1 and 8 of the '385 Patent.

34. In the alternative, Defendant's infringing instrumentalities infringe – at least – claims 1 and 8 of the '385 Patent under the doctrine of equivalents. Defendant's infringing instrumentalities perform substantially the same functions in substantially the same manner with substantially the same structures, obtaining substantially the same results, as the required elements of – at least – claims 1 and 8 of the '385 Patent. Any differences between Defendant's infringing instrumentalities and the claims of the '385 Patent are insubstantial.

35. All recited elements of – at least – claims 1 and 8 of the '385 Patent are present within, or performed by, Defendant's infringing instrumentalities.

36. Defendant's infringing instrumentalities, when used and/or operated in their intended manner or as designed, infringe – at least – claims 1 and 8 of the '385 Patent, and Defendant is therefore liable for infringement of the '385 Patent.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 9,654,617

37. Plaintiff is the owner by assignment of the valid and enforceable United States Patent No. 9,654,617 ("the '617 Patent") entitled "Selectively Providing Content to Users Located Within a Virtual Perimeter" – including all rights to recover for past, present and future acts of infringement. The '617 Patent issued on May 16, 2017, and has a priority date of February 13, 2015. A true and correct copy of the '617 Patent is attached as Exhibit B.

38. Plaintiff herein restates and incorporates by reference paragraphs 11 – 22, above.

39. All recited elements of – at least – claim 1 of the '617 Patent are present within the structure and/or operation of Defendant's infringing instrumentalities.

40. Defendant's infringing instrumentalities comprise a computer program product that comprises a computer readable storage medium having program code stored thereon. That program code is executable by a processor to perform certain operations, as described hereinafter.

41. Defendant's infringing instrumentalities comprise operations that identify a present physical location of a mobile device, based upon wireless communication between the mobile device and at least one beacon.

42. Defendant's infringing instrumentalities determine that the mobile device is located at a particular physical location.

43. Defendant's infringing instrumentalities communicate at least a first message to the mobile device, responsive to determining that the mobile device is located at the particular physical location.

44. Defendant's infringing instrumentalities communicate at least a first message to the mobile device that specifies at least one application to be disabled while the mobile device is present at the physical location.

45. Defendant's infringing instrumentalities receive a response to the first message from the mobile device, indicating that the at least one application is disabled.

46. Defendant's infringing instrumentalities authorize, using a processor, the mobile device to establish presence on a network maintained for the physical location, responsive to the response to the first message.

47. Defendant's infringing instrumentalities infringe – at least – claim 1 of the '617 Patent.

48. Defendant's infringing instrumentalities literally and directly infringe – at least – claim 1 of the '617 Patent.

49. Defendant's infringing instrumentalities perform or comprise all required elements of – at least – claim 1 of the '617 Patent.

50. In the alternative, Defendant's infringing instrumentalities infringe – at least – claim 1 of the '617 Patent under the doctrine of equivalents. Defendant's infringing instrumentalities perform substantially the same functions in substantially the same manner with substantially the same structures, obtaining substantially the same results, as the required elements of – at least – claim 1 of the '617 Patent. Any differences between Defendant's infringing instrumentalities and the claims of the '617 Patent are insubstantial.

51. All recited elements of – at least – claim 1 of the '617 Patent are present within, or performed by, Defendant's infringing instrumentalities.

52. Defendant's infringing instrumentalities, when used and/or operated in their intended manner or as designed, infringe – at least – claim 1 of the '617 Patent, and Defendant is therefore liable for infringement of the '617 Patent.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

a. A judgment in favor of Plaintiff that Defendant has infringed the '385 and '617 Patents;

b. A permanent injunction enjoining Defendant and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in active concert therewith, from infringement of the '385 and '617 Patents;

c. A judgment and order requiring Defendant to pay Plaintiff its damages, costs, expenses, and pre-judgment and post-judgment interest for Defendant's infringement of the '385 and '617 Patents, as provided under 35 U.S.C. § 284;

d. An award to Plaintiff for enhanced damages resulting from the knowing and deliberate nature of Defendant's prohibited conduct with notice being made at least as early as the service date of this complaint, as provided under 35 U.S.C. § 284;

e. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees; and

f. Any and all other relief to which Plaintiff may show itself to be entitled.

September 29, 2022

Respectfully Submitted,

By: /s/ *Ronald W. Burns*

Ronald W. Burns (*Lead Counsel*)
Texas State Bar No. 24031903
Fresh IP, PLC
5900 South Lake Forest Dr., Suite 300
Frisco, Texas 75035
972-632-9009
ron@freship.com

ATTORNEY FOR PLAINTIFF
BACKERTOP LICENSING LLC