COOLEY LLP
HEIDI L. KEEFE (178960)
(hkeefe@cooley.com)
MARK R. WEINSTEIN (193043)
(mweinstein@cooley.com)
MATTHEW J. BRIGHAM (191428)
(mbrigham@cooley.com)
LOWELL D. MEAD (223989)
(lmead@cooley.com)
3175 Hanover Street
Palo Alto, CA 94304-1130
Telephone: (650) 843-5000
Facsimile: (650) 849-7400

COOLEY LLP
MICHAEL G. RHODES (116127)
(rhodesmg@cooley.com)
101 California Street
5th Floor
San Francisco, CA 94111-5800
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

Attorneys for Plaintiff
FACEBOOK, INC.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

FACEBOOK, INC., a Delaware corporation, Plaintiff, v. BLACKBERRY LIMITED, a Canadian corporation, and BLACKBERRY CORPORATION, a Delaware corporation, Defendants.	Case No. 18-5434 **COMPLAINT FOR PATENT INFRINGEMENT** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

1. Plaintiff Facebook, Inc. ("Facebook") submits the following Complaint against BlackBerry Limited ("BlackBerry Ltd.") and BlackBerry Corporation ("BlackBerry Corp.") (collectively, "BlackBerry"):

NATURE OF THE ACTION

2. Facebook brings this action against BlackBerry for infringement of U.S. Patent No. 8,429,231 ("'231 patent"), U.S. Patent No. 7,567,575 ("'575 patent"), U.S. Patent No. 6,356,841 ("'841 patent"), U.S. Patent No. 7,228,432 ("'432 patent"), U.S. Patent No. 6,744,759 ("'759 patent"), and U.S. Patent No. 7,302,698 ("'698 patent") (collectively "the Patents-in-Suit").

FACEBOOK BACKGROUND

3. Facebook's mission is to give people the power to build community and bring the world closer together. Facebook's top priority is to build useful and engaging products that enable people to connect and share with friends and family through mobile devices, personal computers, and other surfaces. Facebook also helps people discover and learn about what is going on in the world around them, enable people to share their opinions, ideas, photos and videos, and other activities with audiences ranging from their closest friends to the public at large, and stay connected everywhere by accessing Facebook's products, including:

- **Facebook**. Facebook enables people to connect, share, discover, and communicate with each other on mobile devices and personal computers. There are a number of different ways to engage with people on Facebook, the most important of which is News Feed which displays an algorithmically-ranked series of stories and advertisements individualized for each person.

- **Instagram**. Instagram is a community for sharing visual stories through photos, videos, and direct messages. Instagram is also a

place for people to stay connected with the interests and communities that they care about.

- **Messenger**. Messenger is a messaging application that makes it easy for people to connect with other people, groups and businesses across a variety of platforms and devices.

- **WhatsApp**. WhatsApp is a fast, simple, and reliable messaging application that is used by people around the world to connect securely and privately.

4. Facebook is also investing in a number of longer-term initiatives, such as connectivity efforts, artificial intelligence research, and augmented and virtual reality, to develop technologies that Facebook believes will help Facebook better serve Facebook's communities and pursue Facebook's mission to give people the power to build community and bring the world closer together.

5. Facebook's product development philosophy is centered on continuous innovation in creating and improving products that are social by design, which means that Facebook's products are designed to place people and their social interactions at the core of the product experience. As Facebook's user base grows, and the level of engagement from the people who use Facebook's products continues to increase, including with video, Facebook's computing needs continue to expand. Facebook makes significant investments in technology both to improve Facebook's existing products and services and to develop new ones, as well as for Facebook's marketers and developers. Facebook is also investing in protecting the security and integrity of Facebook's platform by investing in both people and technology to strengthen Facebook's systems against abuse. Facebook's technology investments included research and development expenses of $7.75 billion, $5.92 billion, and $4.82 billion in 2017, 2016, and 2015, respectively.

6. To establish and protect Facebook's proprietary rights, Facebook relies on a combination of patents, trademarks, copyrights, trade secrets, including know-how, license agreements, confidentiality procedures, non-disclosure agreements with third parties, employee disclosure and invention assignment agreements, and other contractual rights. In addition, to further protect Facebook's proprietary rights, from time to time Facebook has purchased patents and patent applications from third parties.

THE PARTIES

7. Facebook is a corporation organized and existing under the laws of the State of Delaware, having its principal place of business at 1601 Willow Road, Menlo Park, CA 94025.

8. Defendant BlackBerry Ltd. is a corporation organized and existing under the laws of Canada, having its principal place of business at 2200 University Avenue East, Waterloo, Ontario, Canada N2K 0A7.

9. Defendant BlackBerry Corp. is a corporation organized and existing under the laws of the State of Delaware. BlackBerry Corp. operates offices in the Northern District of California, including locations at 3001 Bishop Drive, Suite 400, San Ramon, CA 94583, 331 Fairchild Drive, Suite 300 & 1st Floor, Mountain View, CA 94043, 837 Arnold Drive, Suites 400 & 600, Martinez, CA 94553, and 2988 Campus Drive, Suites 100, 110, 115, and 200, San Mateo, CA 94403.

JURISDICTION

10. This is a civil action for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code. This Court has exclusive subject matter jurisdiction over this complaint pursuant to 28 U.S.C. §§ 1331 and 1338(a).

11. This Court has personal jurisdiction over BlackBerry. Upon information and belief, BlackBerry has committed and continues to commit acts of infringement giving rise to this action within California and within this judicial district. For example, BlackBerry has committed and continues to commit acts of infringement in this District,

by among other things, using, offering for sale, and selling products that infringe the Patents-in-Suit. Furthermore, BlackBerry does substantial business in California and within this District. BlackBerry Corp. is registered to do business in the State of California. BlackBerry Corp. also has offices and employees in California and within this District, including its Principal Executive Office and Principal Business Office in California located at 3001 Bishop Drive, Suite 400, San Ramon, CA 94583. On information and belief, BlackBerry Corp. is a wholly owned subsidiary, directly or indirectly, of BlackBerry Ltd., and BlackBerry Corp. conducts business in this judicial district and in the United States on behalf of BlackBerry Ltd. In conducting business in California and in this judicial district, BlackBerry derives revenue from the infringing products being used, sold, imported, and/or offered for sale and providing service and support to BlackBerry's customers in California and this District.

VENUE

12. Venue is appropriate in the Northern District of California pursuant to 28 U.S.C. §§ 1391(b) and (c) and 1400(b). BlackBerry has committed acts of infringement within this judicial district giving rise to this action. BlackBerry has and continues to conduct business in this District, including one or more acts of selling, using, importing, and/or offering for sale infringing products or providing service to customers in this District. In addition, BlackBerry Corp. has regular and established places of business in this District including the office locations identified above. BlackBerry Ltd. is not a resident of the United States and therefore may be properly sued in this judicial district.

COUNT I: INFRINGEMENT OF U.S. PATENT NO. 8,429,231

13. Facebook incorporates by reference and re-alleges all foregoing paragraphs of this Complaint as if fully set forth herein.

14. Facebook is the owner by assignment of U.S. Patent No. 8,429,231 ("'231 patent"), entitled "Voice Instant Messaging," including the exclusive right to bring suit to enforce the patent and the exclusive right to obtain relief for infringement.

The '231 patent was duly and legally issued by the U.S. Patent and Trademark Office on April 23, 2013. The patent properly claims priority to U.S. Application Ser. No. 09/810,159, filed on March 19, 2001, which claims the benefit of U.S. Provisional Application No. 60/189,974, filed on March 17, 2000, and U.S. Provisional Application No. 60/239,917, filed on October 13, 2000.

15. A true and correct copy of the '231 patent is attached as Exhibit A.

16. The '231 Patent is valid and enforceable under the United States Patent Laws.

SUMMARY OF INVENTION

17. The '231 patent traces its roots to America Online, Inc. ("AOL"). In particular, the written description contained in the '231 patent was originally filed on behalf of AOL with substantially the same content on March 19, 2001. In 2012, Facebook acquired hundreds of patents and related patent application rights that had been previously held by AOL.

18. Before the filing of the patent applications that led to the '231 patent, instant messaging involving the exchange of text messages between senders and recipients was well-known and widely used. The patent's Background section states, for example, that AOL had provided subscribers with the ability to send and receive instant messages and that instant messaging was becoming a preferred means of communicating among online subscribers. ('231, col. 1:33-41.)

19. The inventions of the '231 patent provide techniques and related system functionality for enabling voice communication between users of an instant messaging system. The '231 patent states that the described invention "relates generally to transferring data between subscribers of a communications system and more particularly to transferring audio data between subscribers of an instant messaging host." (*Id.*, col. 1:13-16.) The patent describes the use of multiple communication channels in an instant messaging system to enable voice communication. The patent states, for example: "Voice communication may be enabled by establishing a generic

signaling interface channel, a control channel, and an audio channel between the sender and the recipient." (*Id*., col. 1:64-66.)

20. Among other things, the '231 patent describes that using multiple channels including a generic signaling interface channel can protect users of the communication system, such as by providing for the exchange of local IP addresses only when both users permit the exchange. The patent states, for example: "In one implementation, a talk tool establishes an active talk session using three communication channels: a Generic Signaling Interface (GSI) channel, a control channel, and an audio channel. The talk tool uses the GSI channel to establish the initial connection. During this connection, the local IP addresses are exchanged. After the initial connection phase is done, the GSI channel is no longer used." (*Id*., col. 13:27-33.) The patent further states: "By using the GSI channel, the exchange of local IP addresses is only done when both users permit such an exchange, i.e., by clicking on the CONNECT UI. These actions protect users from having their local EP [*sic*, IP] addresses automatically obtained without their consent." (*Id*., col. 13:27-38.)

21. Consistent with these statements, the claims of the '231 patent recite the use of more than one channel, including a generic signaling interface channel, to establish voice communication between the sender and the recipient. (*See* '231, Claims 1 and 10.)

22. The '231 patent also describes that the instant messaging system can determine the voice communication capabilities of the recipient. The patent states, for example: "Once the instant message is verified, the host **604** determines the capabilities of the recipient (step **615**). For example, the host **604** may monitor and update the online status, client version, and device type of all connected subscribers in real time. The capability to receive audio data may depend on hardware (e.g., device type), software (e.g., client version), and/or transfer preferences (e.g., blocked screen names). To be talk enabled, both the talk software and audio equipment must be available. The host 604 then reports the capabilities of the recipient to the sender (step **620**)." (*Id*., col.

12:16-25.)

23. Consistent with this description, each claim of the '231 patent recites that the invention includes steps or functions of determining voice communication capabilities of the recipient and establishing voice communication "based on the determined voice communication capabilities of the recipient and based on the indication that the sender has selected the voice communication option."

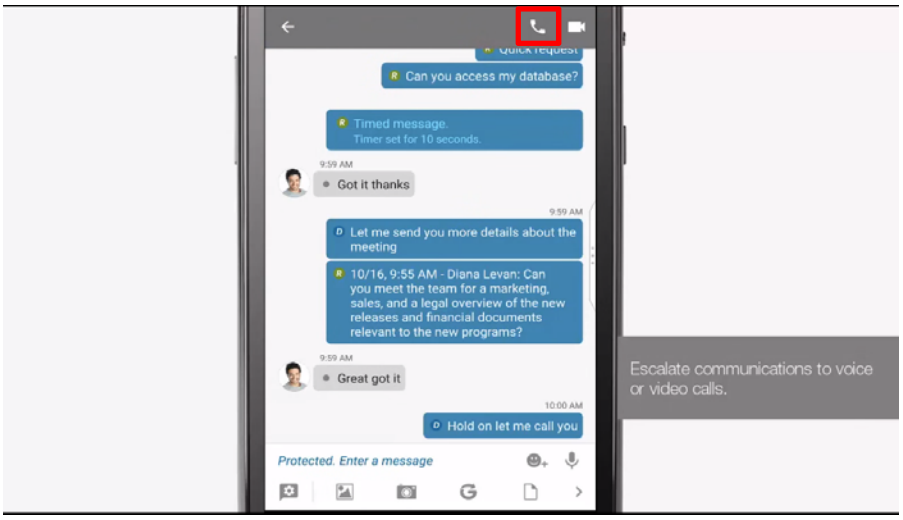
BLACKBERRY'S INFRINGEMENT

24. BlackBerry has infringed and is continuing to infringe the '231 patent by making, using, selling and/or offering to sell in the United States, or importing into the United States, products or processes that practice the '231 patent in violation of 35 U.S.C. § 271(a), including without limitation its BBM Enterprise software product and related functionality.

25. BlackBerry's infringement of the '231 patent has caused and will continue to cause damage to Facebook for which Facebook is entitled to recovery under 35 U.S.C. § 284.

26. As set forth below, BlackBerry infringes the '231 patent. The following description is exemplary and illustrative of BlackBerry's infringement based on publicly available information. Facebook expects to further develop the evidence of BlackBerry's infringement after obtaining discovery from BlackBerry in the course of this action.

27. BBM Enterprise is an instant messaging application and associated system that permits users to exchange text messages and engage in voice and video communications. For example, a user of BBM Enterprise can select a telephone button to initiate a voice call, as shown in the annotated screenshot below.



28. BlackBerry infringes the ’231 patent in connection with BBM Enterprise. The following exemplary figure from the ’231 patent, annotated in red, illustrates how an instant messaging user can initiate voice communication by selecting a button.

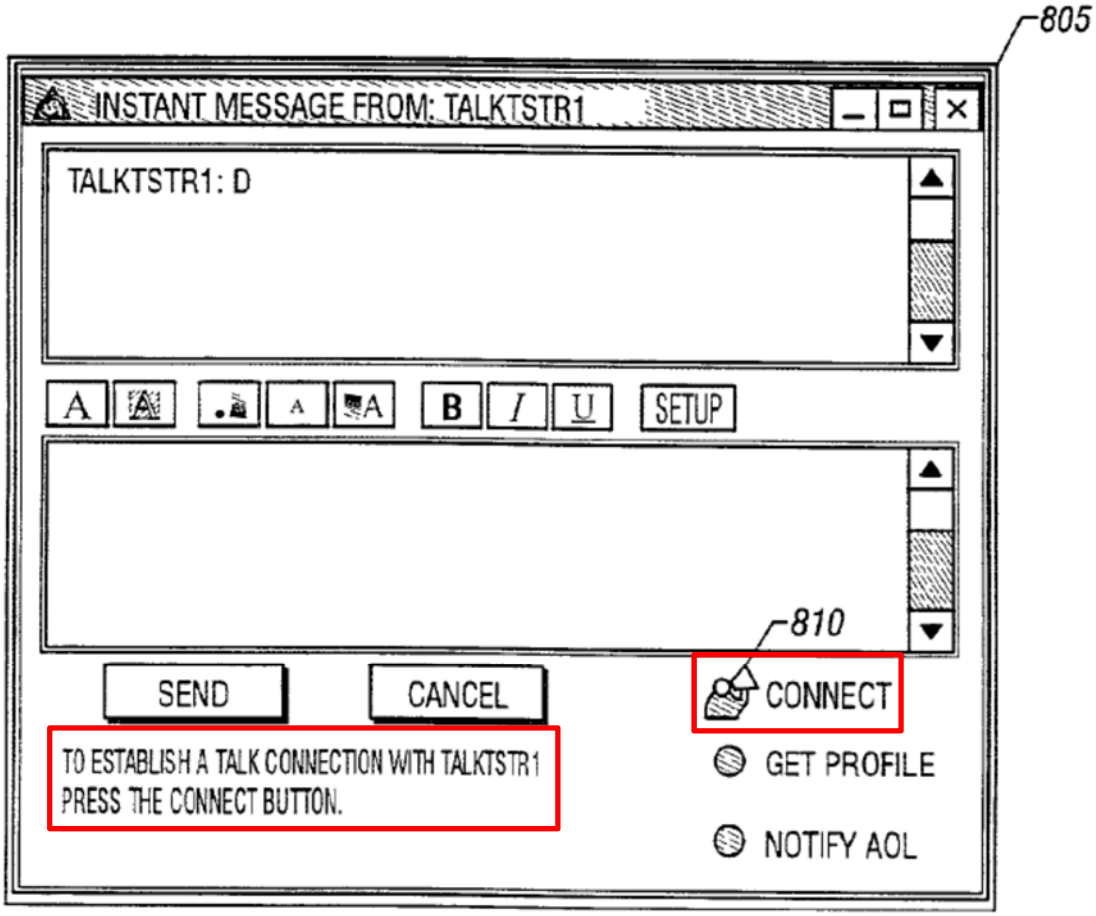


FIG. 8

29. An illustrative description of BlackBerry's infringement on an element-by-element basis is provided below for exemplary claims of the patent.

- *1[p] A method comprising:*

BlackBerry provides BBM Enterprise, which performs the method described below, as used in a variety of different platforms.

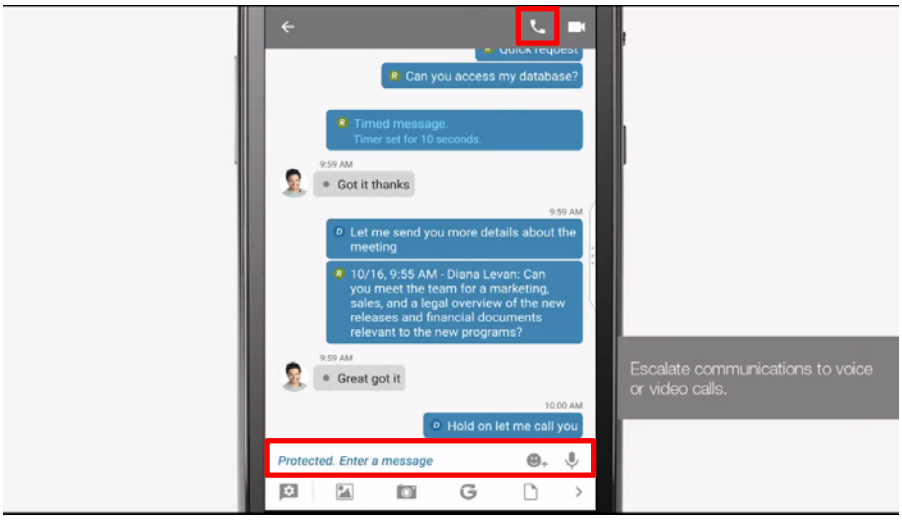
To use BBM Enterprise, you must meet the following requirements:

Device	Requirements
BlackBerry 10 (version 10.3.1 and later)	• Any activation type • Assigned to BBM Enterprise in the Enterprise Identity administrator console • Running BBM Enterprise 20.0 or later • BBM Enterprise user license
iOS (version 8.1 or later)	• Assigned to BBM Enterprise in the Enterprise Identity administrator console • Running BBM Enterprise 1.1 or later • BBM Enterprise user license
Android version 4.3 or later)	• Assigned to BBM Enterprise in the Enterprise Identity administrator console • Running BBM Enterprise 1.1 or later • BBM Enterprise user license
Windows (version 7 and later)	• Assigned to BBM Enterprise in the Enterprise Identity administrator console • Running BBM Enterprise for Windows version 1.0 or later • BBM Enterprise user license
macOS (version 10.7 and later)	• Assigned to BBM Enterprise in the Enterprise Identity administrator console • Running BBM Enterprise for macOS version 1.0 or later • BBM Enterprise user license

(Source: BBM-Enterprise-latest-Security-Note-en.pdf at 6.)

- *[a] enabling presentation of a first communication graphical user interface to a sender, the first communication graphical user interface comprising one or more communication options including a voice communication option;*

BBM Enterprise enables presentation of a first communication graphical user interface to a sender, the first communication graphical user interface comprising one or more communication options including a voice communication option. For example, BBM Enterprise uses a chat interface on the sender's mobile device or computer that presents a sender with an option to send a text message or a voice call.



(Source: BBM Enterprise – Secure Cross-Platform Instant Messaging Demo, at 1:39 (published 10/31/2017) (annotated), available at https://www.youtube.com/watch?v=4AhQS6LYHug.)

Start a BBM Enterprise voice or video chat

You can turn a BBM Enterprise chat into a face-to-face conversation using the video chat feature.

If your device or your contact's device doesn't support video chatting, your call is connected with voice only. Depending on your device, this feature might not be supported.

If your company subscribes to the BBM Protected Voice service, your voice and video chats can be protected. If your voice or video chat is protected, the icon appears on the call screen. If your voice or video chat is not protected, the icon appears on the call screen, and your device will vibrate briefly.

In a chat, in the upper right corner of the screen, tap . Then do one of the following:

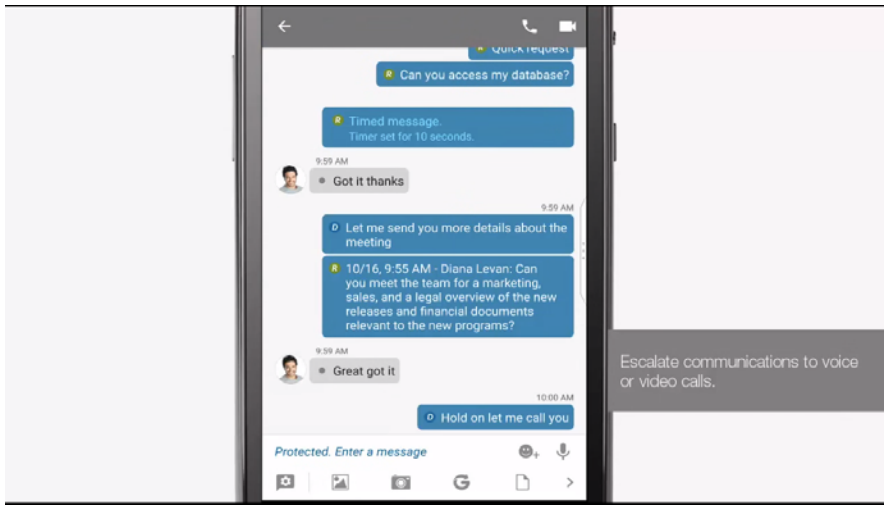
- To start a video chat, tap .
- To start a voice chat, tap .

You can also start a voice or video chat from a contact search. Search for a contact and tap the contact name, then tap .

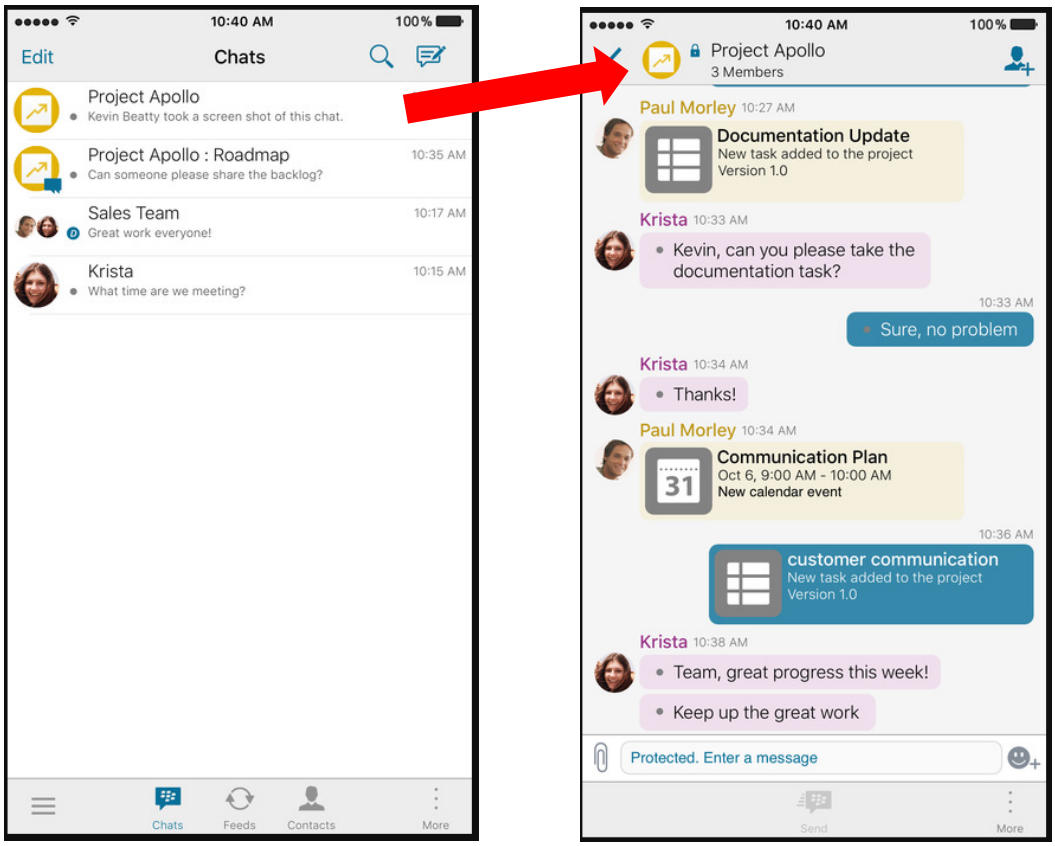
(Source: https://help.blackberry.com/en/bbm-enterprise-for-android/current/help/uvm1474995230203.html)

- *[b] enabling presentation of a second communication graphical user interface to a recipient;*

BBM Enterprise enables presentation of a second communication graphical user interface to a recipient. For example, the recipient of a BBM Enterprise message views the received message in a BBM Enterprise communication interface displayed on the recipient's mobile device or computer.



(Source: BBM Enterprise – Secure Cross-Platform Instant Messaging Demo, at 1:39 (published 10/31/2017), available at https://www.youtube.com/watch?v=4AhQS6LYHug.)



(Source: Apple Store, BBM Enterprise, https://itunes.apple.com/us/app/bbm-enterprise/id1147293419?mt=8 (annotated).)

- *[c] determining voice communication capabilities of the recipient;*

BBM Enterprise determines voice communication capabilities of the recipient. For example, if a recipient can receive voice or video calls, voice and video icons are presented to the sender of a message. In addition, an icon can be shown that identifies that a contact can participate in BBM Voice calls, reflecting that the voice communication capabilities of the contact (potential recipient) have been determined.

Icon	Description
	Tip: Touch and hold the unsent message, and tap to resend it.
	Contact can participate in BBM Voice calls
	Busy status icon

(Source: https://emm.b2b-blackberry.net/dls/Manuals/BBM/PC/BBM_Enterprise_Windows-macOS_1.2.UserGuide-en.pdf)

Start a BBM Enterprise voice or video chat

You can turn a BBM Enterprise chat into a face-to-face conversation using the video chat feature.

If your device or your contact's device doesn't support video chatting, your call is connected with voice only. Depending on your device, this feature might not be supported.

If your company subscribes to the BBM Protected Voice service, your voice and video chats can be protected. If your voice or video chat is protected, the icon appears on the call screen. If your voice or video chat is not protected, the icon appears on the call screen, and your device will vibrate briefly.

In a chat, in the upper right corner of the screen, tap . Then do one of the following:

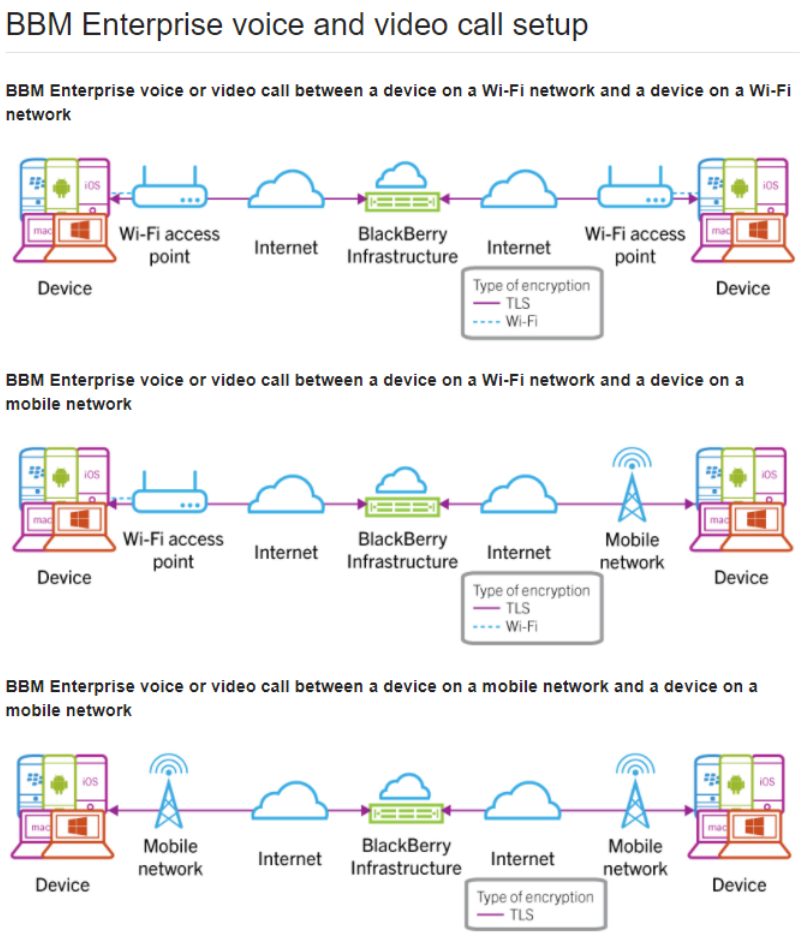
- To start a video chat, tap .
- To start a voice chat, tap .

You can also start a voice or video chat from a contact search. Search for a contact and tap the contact name, then tap .

(Source: https://help.blackberry.com/en/bbm-enterprise-for-android/current/help/uvm1474995230203.html)

- *[d] receiving, at a server, an indication that the sender has selected the voice communication option; and*

BBM Enterprise receives, at a server, an indication that the sender has selected the voice communication option. For example, after a user selects the voice call icon, a BBM Enterprise server receives a request from a sender to set up a voice call with a recipient.

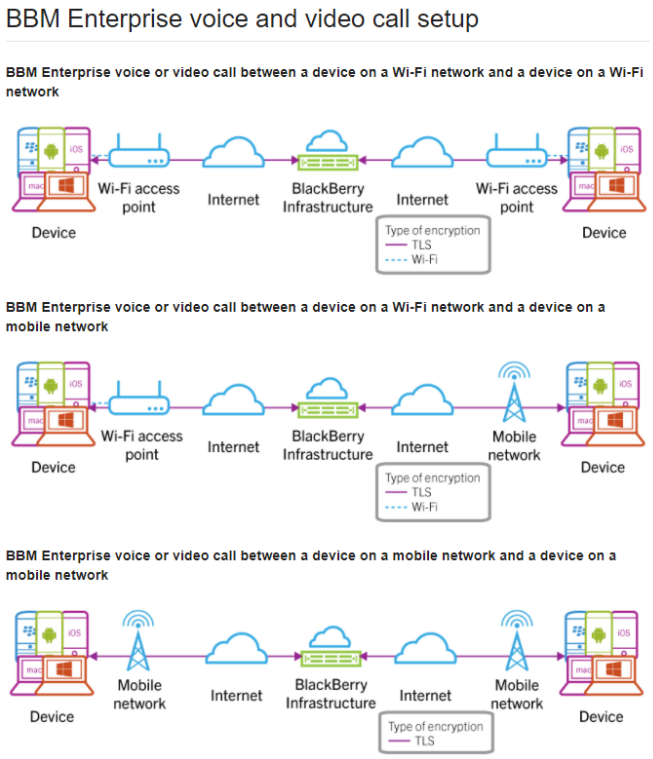


(Source: https://help.blackberry.com/en/bbm-protected-security/latest/bbm-protected-security/sqp1464359148449.html)

- *[e] establishing, based on the determined voice communication capabilities of the recipient and based on the indication that the sender has selected the voice communication option, a voice communication between the sender and the recipient using more than one channel including at least a generic signaling interface channel.*

BBM Enterprise establishes, based on the determined voice communication capabilities of the recipient and based on the indication that the sender has selected the voice communication option, a voice communication between the sender and the recipient using more than one channel including at least a generic signaling interface channel. The establishment of voice communication uses multiple channels including

a generic signaling interface channel. For example, voice communication established between devices on Wi-Fi or cellular networks uses a generic signaling interface channel and may use one or more cellular network channels or Wi-Fi channels. IP addresses may be provided as part of establishing the voice communication. The establishment of voice communication may also use one or more additional channels, such as cellular network control channels as well as a channel through the BlackBerry Infrastructure, which may be an encrypted channel.



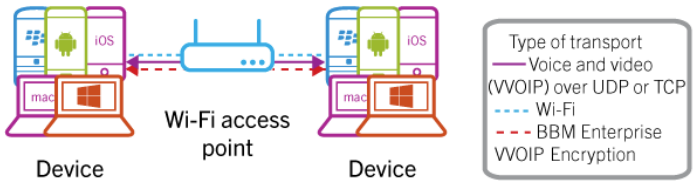
(Source: https://help.blackberry.com/en/bbm-protected-security/latest/bbm-protected-security/sqp1464359148449.html)

BBM Enterprise voice and video call data transfer

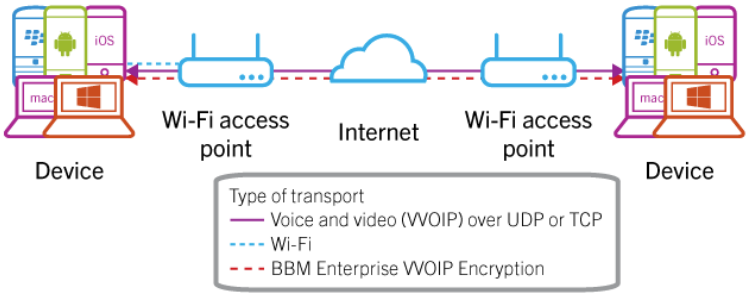
BBM Enterprise voice and video is designed to use the most direct and efficient path for data transfer between the two users in the call. In some cases, when a direct path is not possible, the encrypted voice or video call will be connected through the BlackBerry Infrastructure.

Note: BlackBerry OS devices are not capable of conducting secure BBM Enterprise voice and video calls.

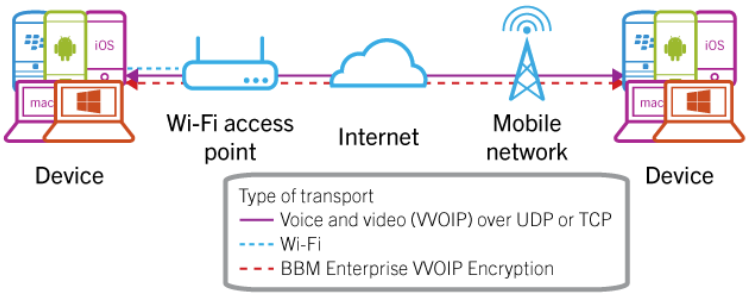
BBM Enterprise voice or video call between devices on the same Wi-Fi network



BBM Enterprise voice or video call between a device on a Wi-Fi network and a device on a different Wi-Fi network

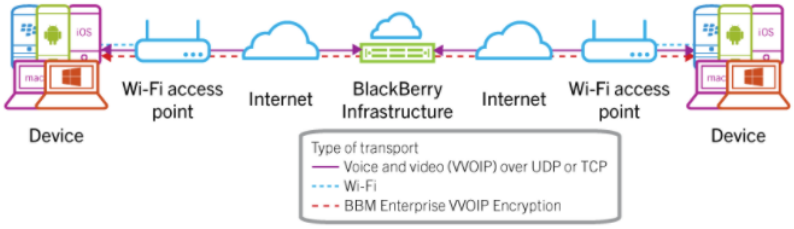


BBM Enterprise voice or BBM Video between a device on a Wi-Fi network and a device on a mobile network

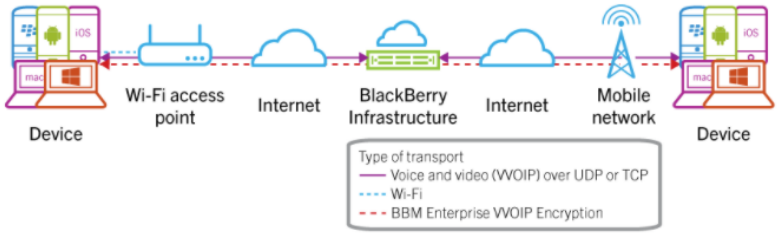


BBM Enterprise voice or BBM Video between a device on a mobile network and a device on a mobile network

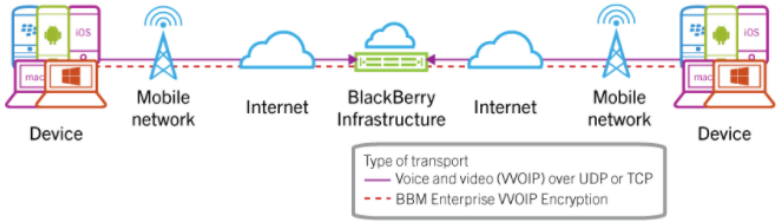
BBM Enterprise video or voice between a device on a Wi-Fi network and a device on a Wi-Fi network through the BlackBerry Infrastructure



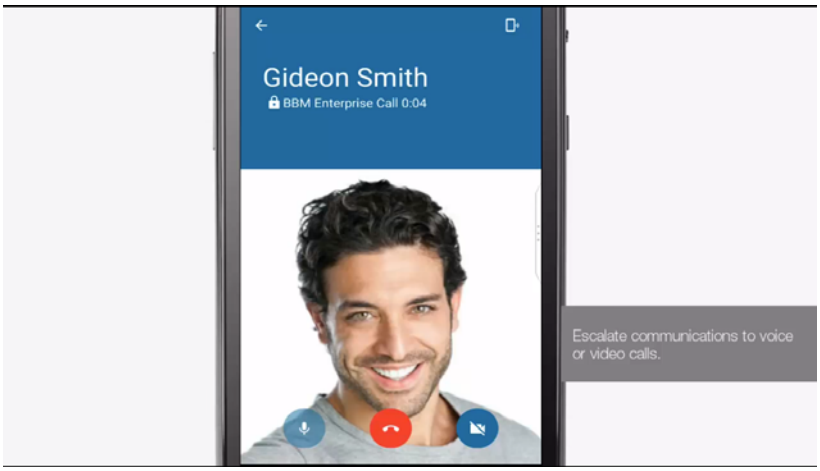
BBM Enterprise video or voice between a device on a Wi-Fi network and a device on a mobile network through the BlackBerry Infrastructure



BBM Enterprise video or voice between a device on a mobile network and a device on a mobile network through the BlackBerry Infrastructure



(Source: https://help.blackberry.com/en/bbm-protected-security/latest/bbm-protected-security/zgh1464359194884.html)



(Source: BBM Enterprise – Secure Cross-Platform Instant Messaging Demo, at 1:48 (published 10/31/2017) (annotated), available at https://www.youtube.com/watch?v=4AhQS6LYHug.)

- *3. The method of claim 1, wherein determining voice communication capabilities of the recipient comprises determining whether the recipient has enabled a hardware device for voice communication.*

As explained with respect to Claim 1[c], BBM Enterprise determines voice communication capabilities of the recipient comprising determining whether the recipient has enabled a hardware device for voice communication. For example, BBM Enterprise determines whether the recipient's device hardware and/or software supports voice communication.

- *4. The method of claim 1, wherein determining voice communication capabilities of the recipient comprises determining whether the recipient has enabled software for voice communication.*

As explained with respect to Claim 1[c], BBM Enterprise determines voice communication capabilities of the recipient comprising determining whether the recipient has enabled software for voice communication. For example, BBM Enterprise determines whether the recipient's device hardware and/or software supports voice communication.

- *6. The method of claim 1, further comprising reporting the voice*

communication capabilities of the recipient to the sender.

BBM Enterprise reports the voice communication capabilities of the recipient to the sender. For example, BBM Enterprise displays voice and video call icons if the recipient has voice and video call capability, as discussed with respect to Claim 1[c].

- *9. The method of claim 1, wherein the more than one channel further comprises a different communications channel than a control channel associated with instant message communications between the sender and the recipient.*

BBM Enterprise uses more than one channel including a different communication channel than a control channel associated with instant message communications between the sender and recipient. For example, on information and belief, a control channel is used for the text instant messaging in BBM Enterprise that is different from a voice communications channel.

30. Facebook is entitled to relief as a result of BlackBerry's infringement, including without limitation monetary damages no less than a reasonable royalty.

COUNT II: INFRINGEMENT OF U.S. PATENT NO. 7,567,575

31. Facebook incorporates by reference and re-alleges all foregoing paragraphs of this Complaint as if fully set forth herein.

32. Facebook is the owner by assignment of U.S. Patent No. 7,567,575 ("'575 patent"), entitled "Personalized multimedia services using a mobile service platform," including the exclusive right to bring suit to enforce the patent and the exclusive right to obtain relief for infringement. The '575 patent was duly and legally issued by the U.S. Patent and Trademark Office on July 28, 2009. The patent is based on U.S. Patent Application Ser. No. 10/136,540 filed on May 1, 2002, and claims the benefit of U.S. Provisional Application No. 60/317,712, filed on Sep. 7, 2001.

33. A true and correct copy of the '575 patent is attached as Exhibit B.

34. The '575 patent is valid and enforceable under the United States Patent Laws.

SUMMARY OF INVENTION

35. The '575 patent originated with AT&T Corp. ("AT&T"), as reflected on the face of the patent. At the time of the patent filing, AT&T identified itself as among the world's premier voice, video, and data communications companies, serving consumers, businesses, and government. Backed by the research and development capabilities of AT&T Labs, AT&T ran the world's largest, most sophisticated communications network, was the largest cable operator in the U.S., was a leading supplier of data and Internet services for businesses, and offered outsourcing, consulting and networking-integration to large businesses, according to the company.

36. Before the filing of the '575 patent, users of mobile devices could access content on the Internet over a wireless connection. (*See* '575, col. 1:24-49.) However, according to the '575 patent, accessing multimedia data on the Internet from a mobile device over a wireless connection was often unreliable and could suffer from congestion and problematic transmission conditions. For example, according to the patent, "[w]ireless access links suffer from severe transmission conditions, such as narrow bandwidth, higher bit error rates and high latency." (*Id*., col. 2:12-14.) "Another problem with wireless links is congestion of the control and request channels when these channels are used simultaneously to deliver the multimedia content." (*Id*., col. 2:22-25.) According to the '575 patent, "[i]t would, therefore, be desirable to provide personal multimedia services delivered over a wireless communication channel to a variety of mobile device types while minimizing congestion of the control and request paths. It would further be desirable to provide a mobile service platform and separate multimedia servers having distinct channels for delivering transcoded multimedia data and adapting the delivery of the multimedia data to fluctuations of the wireless communication channel conditions." (*Id*., col. 2:26-34.)

37. The invention of the '575 patent addresses these perceived needs. The invention provides a mobile platform to deliver multimedia (for example, graphics, video, and/or audio) with a request path and control channel to minimize congestion

while leveraging the identity of the mobile user and a profile of the mobile device. The patent identifies a number of technological improvements to computer network functionality that flow from the invention, such as the following:

- "In one aspect of the invention, a method for providing multimedia data from at least one controllable multimedia source to a mobile device includes providing a request path from the mobile device to a mobile service platform, receiving a request from the mobile device, obtaining a device profile from the mobile device, authenticating the identity of a user of the mobile device, and determining a user profile in response to the user identity. The method further includes authorizing control and access to the at least one multimedia source, providing a control channel from the mobile service platform to at least one multimedia server, providing multimedia data delivery information to the at least one multimedia server, and providing multimedia data to the mobile device in response to the request via the at least one multimedia server. With such a technique, personal multimedia services are delivered over a wireless communication channel to a variety of mobile device types while minimizing congestion of the control and request paths, and a mobile user can control multimedia sources over the wireless channel. By routing the control paths through the mobile service platform and the content delivery paths through multimedia servers, the control, transcoding, and multimedia delivery functions are handled efficiently without overloading any particular communications pipe. The inventive technique enables different modes of communication from a multitude of handheld devices for efficient and personalized multimedia delivery." (*Id.*, col. 2:60-3:18.)

- "In general, the present invention provides personalized multimedia service by integrating a mobile service platform, and a plurality of multimedia servers for wireless multimedia delivery. The mobile service platform operates as a message gateway for allowing mobile devices using various protocols on different access networks to access multimedia resources on the Internet and various other networks. The mobile service platform includes a flexible architecture having a plurality of

components that cooperate to service mobile device service requests." (*Id.*, col. 4:19-28.)

38. The claims of the '575 patent, which includes claim 1 and the claims that depend from claim 1, reflect these technological benefits to computer network functionality. Claim 1 recites a method for providing multimedia data from at least one controllable source to a mobile device, consistent with the specification's descriptions for personalized multimedia data delivery where a mobile user can control multimedia sources. As described in the specification, by using the inventive technique for authorizing control and access to the at least one multimedia source, providing a control channel from the mobile service platform to at least one multimedia server, providing multimedia data delivery information to the at least one multimedia server, and providing multimedia data to the mobile device in response to the request via the at least one multimedia server, as reflected in claim 1, personal multimedia services can be delivered over a wireless communication channel to a variety of mobile device types while minimizing congestion of the control and request paths, and a particular mobile user can exercise control over multimedia sources through the wireless channel.

39. Claim 1 further recites steps including providing a request path from the mobile device to a mobile service platform, providing a control channel from the mobile service platform to at least one multimedia server, and providing multimedia data to the mobile device via the at least one multimedia server. These features of claim 1 further reflect the specification's teachings that by routing the control paths through the mobile service platform and the content delivery paths through multimedia servers, the control and multimedia delivery functions are handled efficiently without overloading any particular communications pipe, and that the inventive technique enables different modes of communication from a multitude of handheld devices for efficient and personalized multimedia delivery.

40. Furthermore, claim 1 recites steps of obtaining a device profile, authenticating the identity of a user of the mobile device, determining a user profile

corresponding to the user identity, and authorizing control and access to the at least one multimedia source. These features reflect the specification's descriptions of how the invention provides benefits including personal multimedia services and personalized multimedia delivery.

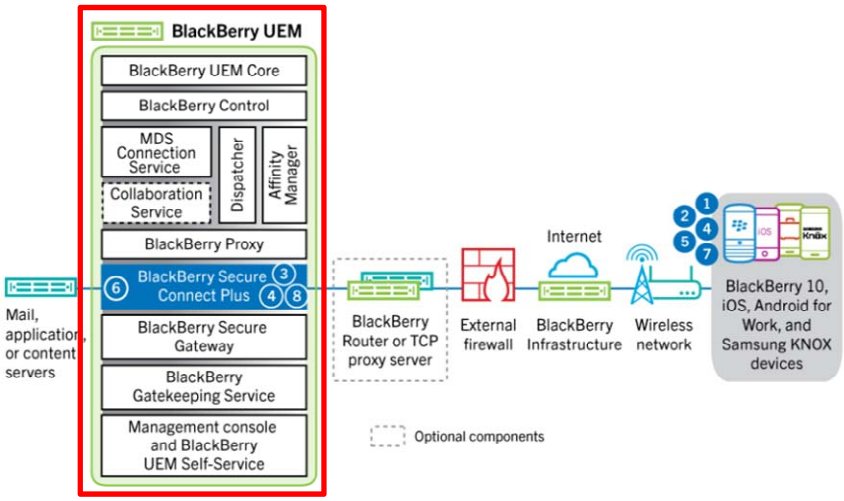
BLACKBERRY'S INFRINGEMENT

41. BlackBerry has infringed and is continuing to infringe the '575 patent by making, using, selling and/or offering to sell in the United States, or importing into the United States, products or processes that practice the '575 patent in violation of 35 U.S.C. § 271(a), including without limitation its BlackBerry UEM (Unified Endpoint Manager) product and related functionality, which were formerly named BlackBerry Enterprise Server (BES) in various versions, including its implementation with BlackBerry's Secure Connect Plus product and related functionality.

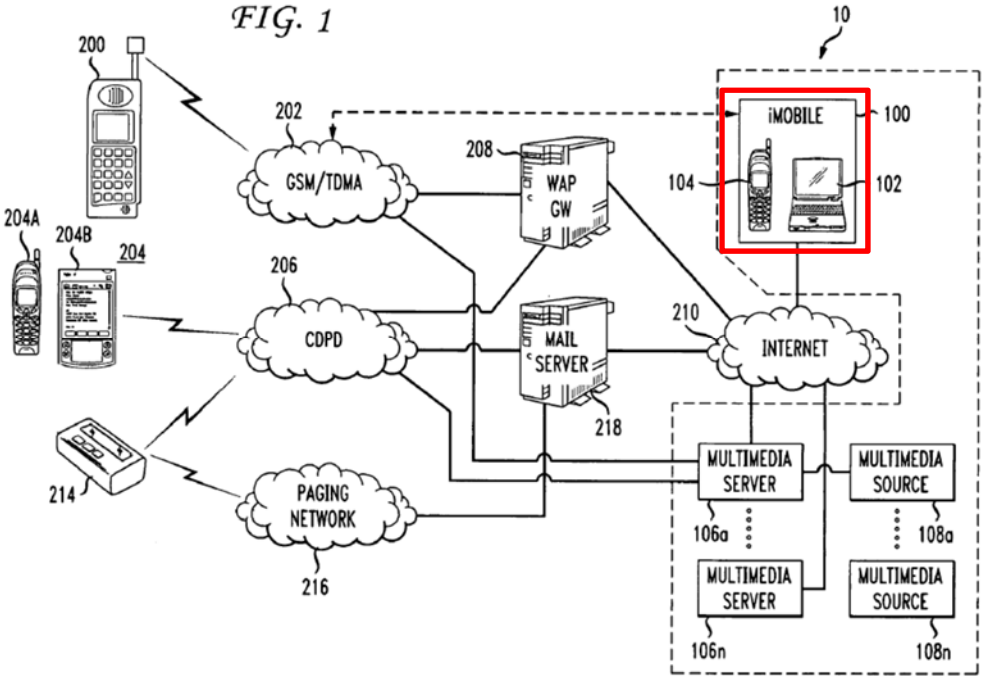
42. BlackBerry's infringement of the '575 patent has caused and will continue to cause damage for which Facebook is entitled to recovery under 35 U.S.C. § 284.

43. As set forth below, BlackBerry infringes the '575 patent. The following description is exemplary and illustrative of BlackBerry's infringement based on publicly available information. Facebook expects to further develop the evidence of BlackBerry's infringement after obtaining discovery from BlackBerry in the course of this action.

44. The BlackBerry UEM product provides endpoint management and policy control for devices and apps. BlackBerry provides a cloud-based solution hosted by BlackBerry. BlackBerry Secure Connect Plus is a BlackBerry UEM component that provides a secure IP tunnel between apps and an organization's network. A network architecture illustration by BlackBerry is provided below, with the red annotation added.



45. An illustrative figure from the '575 patent is provided below, with the red annotation added around an exemplary mobile service platform.



46. An illustrative description of BlackBerry's infringement on an element-by-element basis is provided below for exemplary claims of the patent.

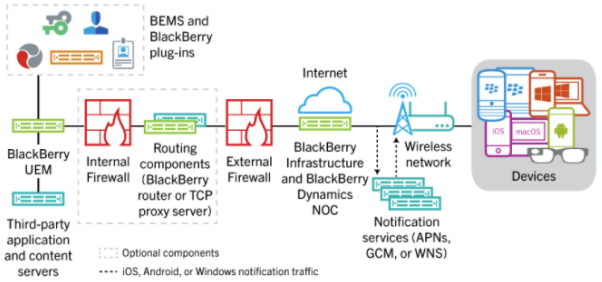
- *1[p] A method for providing multimedia data from at least one controllable multimedia source to a mobile device comprising:*

BlackBerry UEM, including its implementation with Secure Connect Plus, provides for the secure transfer of data between the source and the device. According to BlackBerry, UEM helps "[s]ecure and manage mobile devices, laptops and other endpoints across different operating systems and ownership models. Control user access to business apps, data and content. And do it all from a single, easy-to-use management console, with an extensive set of policies and profiles to suit your needs." (Source: https://us.blackberry.com/content/dam/blackberry-com/PDF/enterprise/ds-blackberry-uem.pdf)

BlackBerry UEM Architecture and data flows

The BlackBerry UEM architecture was designed to help you manage mobile devices for your organization and provide a secure link for data to travel between your organization's mail and content servers and your user's devices.

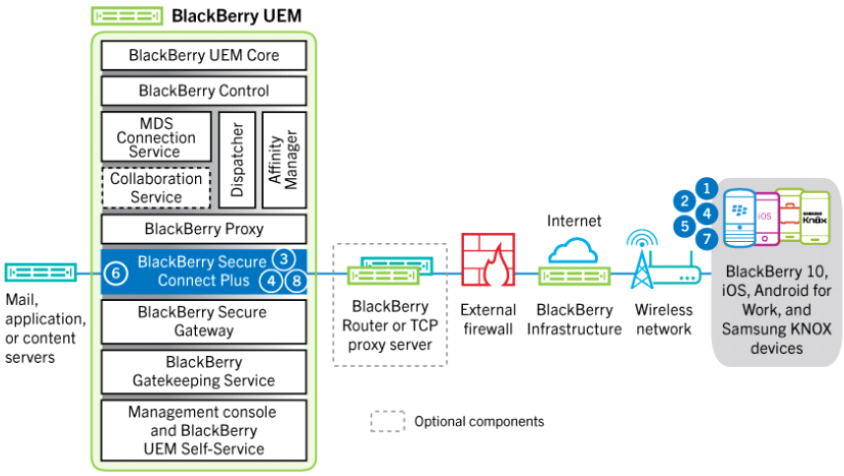
Architecture: BlackBerry UEM solution



Component	Description
BlackBerry UEM	BlackBerry UEM is a unified endpoint management solution that provides comprehensive multiplatform device, application, and content management with integrated security and connectivity.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/architecture/ake1452094272560.html)

Data flow: Accessing an application or content server using BlackBerry Secure Connect Plus



(Source: http://help.blackberry.com/en/blackberry-uem/current/architecture/lsh1428958213732.html)

2. The device sends a requests through a TLS tunnel, over port 443, to the BlackBerry Infrastructure to request a secure tunnel to the work network. The signal is encrypted by default using FIPS-140 certified Certicom libraries. The signaling tunnel is encrypted end-to-end.

3. BlackBerry Secure Connect Plus receives the request from the BlackBerry Infrastructure through port 3101.

4. The device and BlackBerry Secure Connect Plus negotiate the tunnel parameters and establish a secure tunnel for the device through the BlackBerry Infrastructure. The tunnel is authenticated and encrypted end-to-end with DTLS.

5. The app uses the tunnel to connect to the application or content server using standard IPv4 protocols (TCP and UDP).

6. BlackBerry Secure Connect Plus transfers the IP data to and from your organization's network. BlackBerry Secure Connect Plus encrypts and decrypts traffic using FIPS-140 certified Certicom libraries.

7. The app receives and displays the data on the device.

8. As long as the tunnel is open, supported apps use it to access network resources. When the tunnel is no longer the best available method to connect to your organization's network, BlackBerry Secure Connect Plus terminates it.

(Source: http://help.blackberry.com/en/blackberry-uem/current/architecture/lsh1428958213732.html)

- *[a] providing a request path from the mobile device to a mobile service platform;*

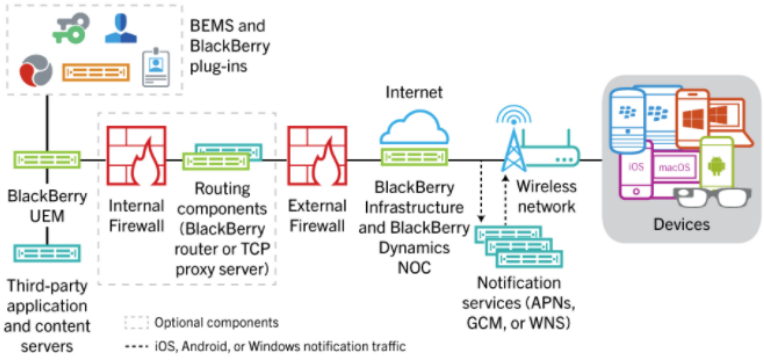
BlackBerry UEM, including implementations with Secure Connect Plus, includes functionality that allows a mobile device to request secure access to data from

the user's organization. In order for a mobile device to access the data through BlackBerry UEM, the user may activate their device using a supplied username and password. For many types of devices, this activation is done through the UEM Client application in communication with the UEM server, which may be a cloud implementation. UEM provides a request path from the user's device to the mobile service platform in the cloud. The request path passes between the mobile device and the organizational content through BlackBerry's UEM architecture.

BlackBerry UEM Architecture and data flows

The BlackBerry UEM architecture was designed to help you manage mobile devices for your organization and provide a secure link for data to travel between your organization's mail and content servers and your user's devices.

Architecture: BlackBerry UEM solution

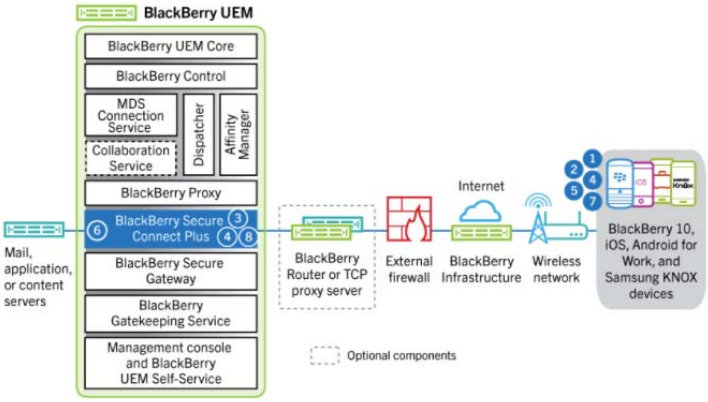


Component	Description
BlackBerry UEM	BlackBerry UEM is a unified endpoint management solution that provides comprehensive multiplatform device, application, and content management with integrated security and connectivity.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/architecture/ake1452094272560.html)

BlackBerry Infrastructure	The BlackBerry Infrastructure registers user information for device activation, validates licensing information for BlackBerry UEM, and provides a trusted path between the organization and every user based on strong, cryptographic, mutual authentication. BlackBerry UEM maintains a constant connection to the BlackBerry Infrastructure, meaning that organizations require only a single outbound connection to a trusted IP address to send data to users. All the data that travels between the BlackBerry Infrastructure and BlackBerry UEM is authenticated and encrypted to provide a secure communication channel into your organization for devices outside the firewall.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/architecture/ake1452094272560.html)



1. The user opens an app to access work data from a content or application server behind your organization's firewall.
   - For BlackBerry 10 devices and Android devices with a work profile, all work space apps use BlackBerry Secure Connect Plus.
   - For iOS devices, you specify whether all apps or only specified apps use BlackBerry Secure Connect Plus.
   - For Android devices with a work profile, all work space apps except those you choose to restrict use BlackBerry Secure Connect Plus.
   - For Samsung KNOX Workspace devices, you specify whether all work space apps or only specified work apps use BlackBerry Secure Connect Plus.
2. The device sends a requests through a TLS tunnel, over port 443, to the BlackBerry Infrastructure to request a secure tunnel to the work network. The signal is encrypted by default using FIPS-140 certified Certicom libraries. The signaling tunnel is encrypted end-to-end.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/architecture/ake1452094272560.html)

The BlackBerry UEM Client is an app that lets users activate devices on BlackBerry UEM. The UEM Client is required to activate the following devices:

- iOS
- Android, including Android wearable devices
- Windows Phone 8

Users can download the UEM Client from the App Store, Google Play, or Windows Store.

The following table summarizes the functions of the UEM Client:

BlackBerry UEM Client function	Description
Communication with BlackBerry UEM	The UEM Client allows BlackBerry UEM to communicate with devices for the purpose of device activation and device management. For more information about activation data flows, see the Architecture content.

(Source: http://help.blackberry.com/en/blackberry-uem/current/administration/blackberry-uem-client.html)

- *[b] receiving a request from the mobile device;*

BlackBerry UEM includes functionality that receives requests from mobile devices, such as a request to permit the device to obtain a secure connection between the device and an organization's apps or related content.

The BlackBerry UEM Client is an app that lets users activate devices on BlackBerry UEM. The UEM Client is required to activate the following devices:

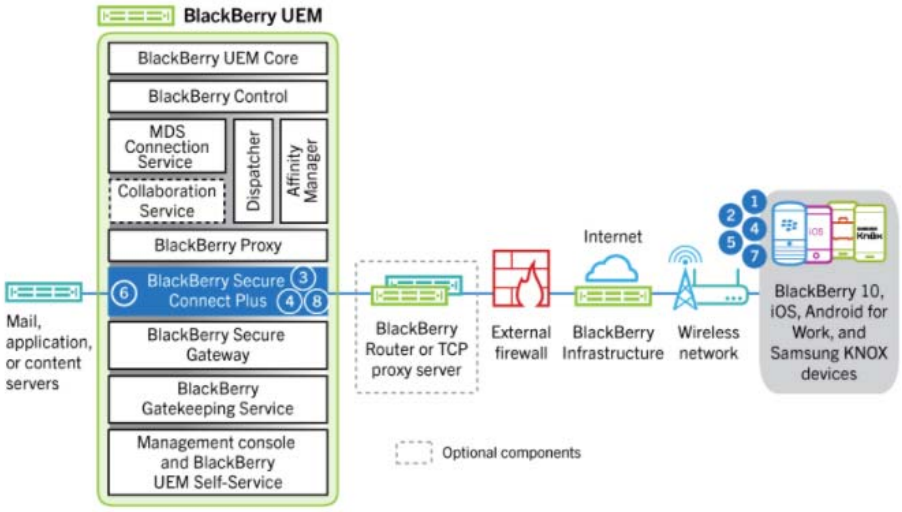
- iOS
- Android, including Android wearable devices
- Windows Phone 8

Users can download the UEM Client from the App Store, Google Play, or Windows Store.

The following table summarizes the functions of the UEM Client:

BlackBerry UEM Client function	Description
Communication with BlackBerry UEM	The UEM Client allows BlackBerry UEM to communicate with devices for the purpose of device activation and device management. For more information about activation data flows, see the Architecture content.

(Source: http://help.blackberry.com/en/blackberry-uem/current/administration/blackberry-uem-client.html)



2. The device sends a requests through a TLS tunnel, over port 443, to the BlackBerry Infrastructure to request a secure tunnel to the work network. The signal is encrypted by default using FIPS-140 certified Certicom libraries. The signaling tunnel is encrypted end-to-end.

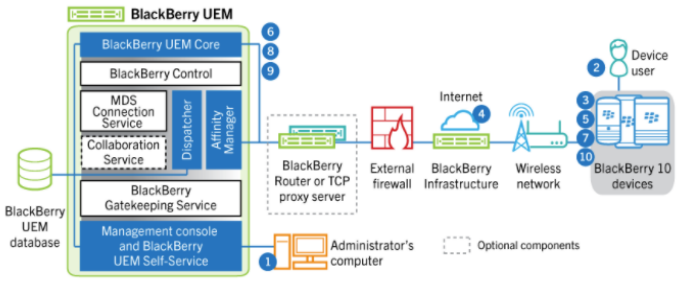
3. BlackBerry Secure Connect Plus receives the request from the BlackBerry Infrastructure through port 3101.

(Source: http://help.blackberry.com/en/blackberry-uem/current/architecture/lsh1428958213732.html)

- *[c] obtaining a device profile from the mobile device;*

In order to activate a device and establish a connection on BlackBerry UEM, a mobile device is required to send certain information to BlackBerry UEM, including sending encrypted CSR and HMAC information. On information and belief, in connection with requesting information from a remote source, the mobile device also transmits device profile data (information about the mobile device) to the UEM server or cloud implementation, such as the device type, operating system, and/or other profile information.

Data flow: Activating a BlackBerry 10 device



5. The device performs the following actions:

a. Establishes a connection with BlackBerry UEM

b. Generates a shared symmetric key that is used to protect the CSR and response BlackBerry UEM using the activation password and EC-SPEKE.

c. Creates an encrypted CSR and HMAC as follows:

- Generates a key pair for the certificate
- Creates a PKCS#10 CSR that includes the public key of the key pair
- Encrypts the CSR using the shared symmetric key and AES-256 in CBC mode with PKCS#5 padding
- Computes an HMAC of the encrypted CSR using SHA-256 and appends it to the CSR

d. Sends the encrypted CSR and HMAC to BlackBerry UEM

8. BlackBerry UEM performs the following actions:

   a. BlackBerry UEM Core assigns the new device to a BlackBerry UEM instance in the domain

   b. BlackBerry UEM Core notifies the active BlackBerry Affinity Manager that a new device is assigned to the BlackBerry UEM instance

   c. The active BlackBerry Affinity Manager notifies the BlackBerry Dispatcher on that BlackBerry UEM instance that there is a new device

   d. The BlackBerry UEM Core sends configuration information, including enterprise connectivity settings to the device

9. BlackBerry UEM Core and the device generate the device transport key using ECMQV and the authenticated long-term public keys from the client certificate and the server certificate for BlackBerry UEM. This key is used to encrypt work data when not using BlackBerry Secure Connect Plus and push to IPPP data.

10. The device sends an acknowledgment over TLS to BlackBerry UEM to confirm that it received and applied the IT policy and other data and created the work space. The activation process is complete.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/architecture/kja1394733078938.html)

Creating activation profiles

You can control how devices are activated and managed using activation profiles. An activation profile specifies how many and what types of devices a user can activate and the type of activation to use for each device type.

The activation type allows you to configure how much control you have over activated devices. You might want complete control over a device that you issue to a user. You might want to make sure that you have no control over the personal data on a device that a user owns and brings to work.

The assigned activation profile applies only to devices the user activates after you assign the profile. Devices that are already activated are not automatically updated to match the new or updated activation profile.

When you add a user to BlackBerry UEM, the Default activation profile is assigned to the user account. You can change the Default activation profile to suit your requirements, or you can create a custom activation profile and assign it to users or user groups.

Activation profiles do not apply to BlackBerry OS (version 5.0 to 7.1) devices.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/administration/activation-profile.html)

Device activation

When you activate a device, you associate the device with BlackBerry UEM so that you can manage devices and users can access work data on their devices.

When a device is activated, you can send IT policies and profiles to control the available features and manage the security of work data. You can also assign apps for the user to install. Depending on how much control the selected activation type allows, you may also be able to protect the device by restricting access to certain data, remotely setting passwords, locking the device, or deleting data.

You can assign activation types to accommodate the requirements of devices owned by your organization and devices owned by users. Different activation types give you different degrees of control over the work and personal data on devices, ranging from full control over all data to specific control over work data only.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/administration/activating_devices.html)

Getting started with BlackBerry UEM Client

You use the BlackBerry UEM Client to activate your device for work. When you activate your device, the device is associated with BlackBerry UEM and is granted access to work data and the productivity apps that your administrator assigned to your device. Your administrator determines the degree of protection for your device based on your role and assigns IT policies and profiles to make sure the appropriate device features are available to you and to secure work data on your device.

You can download the BlackBerry UEM Client for Android devices from the Google Play store.

(Source: http://help.blackberry.com/en/blackberry-uem-client-for-android/current/user-guide/mws1480630841555.html)

Creating device groups

A device group is a group of devices that have common attributes, such as device model and manufacturer, OS type and version, service provider, and whether the device is owned by your organization or by the user. BlackBerry UEM automatically moves devices into or out of the device group based on the device attributes that you define.

You can use device groups to apply different sets of policies, profiles, and apps to devices assigned to a single user. For example, you can use a device group to apply a specific IT policy to all devices running BlackBerry 10 OS, or to all HTC EVO devices running Android OS 4.0 or later on the T-Mobile network.

Policies, profiles, and apps assigned to a device group take priority over those assigned to a user or a user group. However, you cannot assign activation profiles or user certificates to device groups.

Device groups do not include BlackBerry OS (version 5.0 to 7.1) devices. Even if you create a device group query that would logically include your BlackBerry OS devices, they are not included in the device group.

(Source: http://help.blackberry.com/en/blackberry-uem/current/administration/creating-a-device-group.html)

- *[d] authenticating the identity of a user of the mobile device;*

BlackBerry UEM requires a user to activate the user's device before accessing the secure network. This activation process requires an assigned username and password, or the work email and password associated with the user. This information required for activation authenticates the identity of the user. In addition, the UEM server or cloud implementation authenticates the identity of the user of the mobile device in connection with requests from the mobile device to the cloud implementation. According to BlackBerry, the BlackBerry Infrastructure provides a trusted path between the organization and every user based on mutual authentication.

An Enhanced User Experience

BlackBerry UEM opens a world of choice for your users. With support for a wide array of platforms, including iOS, Android, Windows 10, macOS and BlackBerry, your employees can use the tools they prefer for productivity, without sacrificing security. A consistent, user-friendly enrollment process ensures that your users can quickly and securely gain access to essential work apps and resources. And a unified self-service portal enables your employees to easily complete common tasks, such as activating new devices or business apps, without having to depend on IT assistance.

(Source: https://us.blackberry.com/content/dam/blackberry-com/PDF/enterprise/ds-blackberry-uem.pdf)

Industry-Leading Enterprise Security

For enhanced security, BlackBerry UEM offers comprehensive management for native container solutions such as Android™ for Work and Samsung Knox Workspace, in addition to native protection capabilities such as iOS Managed App Configuration and Windows Information Protection. And to help your employees stay productive on the go, BlackBerry® Connectivity, powered by BlackBerry's global secure communications infrastructure, securely extends mobile access to work resources located behind the firewall – without a separate VPN.

(Source: https://us.blackberry.com/content/dam/blackberry-com/PDF/enterprise/ds-blackberry-uem.pdf)

Device activation

When you activate a device, you associate the device with BlackBerry UEM so that you can manage devices and users can access work data on their devices.

When a device is activated, you can send IT policies and profiles to control the available features and manage the security of work data. You can also assign apps for the user to install. Depending on how much control the selected activation type allows, you may also be able to protect the device by restricting access to certain data, remotely setting passwords, locking the device, or deleting data.

You can assign activation types to accommodate the requirements of devices owned by your organization and devices owned by users. Different activation types give you different degrees of control over the work and personal data on devices, ranging from full control over all data to specific control over work data only.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/administration/activating_devices.html)

BlackBerry Infrastructure	The BlackBerry Infrastructure registers user information for device activation, validates licensing information for BlackBerry UEM, and provides a trusted path between the organization and every user based on strong, cryptographic, mutual authentication. BlackBerry UEM maintains a constant connection to the BlackBerry Infrastructure, meaning that organizations require only a single outbound connection to a trusted IP address to send data to users. All the data that travels between the BlackBerry Infrastructure and BlackBerry UEM is authenticated and encrypted to provide a secure communication channel into your organization for devices outside the firewall.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/architecture/ake1452094272560.html)

- *[e] determining a user profile corresponding to the user identity;*

Once a device has been activated with BlackBerry UEM using a username and password assigned to the user, and when a user's mobile device seeks access through the network, the system can determine that a user profile has been created. This user account allows the administrator to assign IT policies and profiles to make sure the appropriate features are available to the user.

An Enhanced User Experience

BlackBerry UEM opens a world of choice for your users. With support for a wide array of platforms, including iOS, Android, Windows 10, macOS and BlackBerry, your employees can use the tools they prefer for productivity, without sacrificing security. A consistent, user-friendly enrollment process ensures that your users can quickly and securely gain access to essential work apps and resources. And a unified self-service portal enables your employees to easily complete common tasks, such as activating new devices or business apps, without having to depend on IT assistance.

(Source: https://us.blackberry.com/content/dam/blackberry-com/PDF/enterprise/ds-blackberry-uem.pdf)

Users and groups

You can create user accounts and then create groups of users to help manage users and devices efficiently.

(Source: http://help.blackberry.com/en/blackberry-uem/current/administration/managing_user_groups_and_user_accounts.html)

Creating and managing user accounts

You can add user accounts directly to BlackBerry UEM or, if you connected BlackBerry UEM to your company directory, you can add user accounts from your company directory. For information about connecting BlackBerry UEM to a company directory and enabling directory-linked groups, see the Configuration content.

You can also use a .csv file to add multiple user accounts to BlackBerry UEM at the same time.

(Source: http://help.blackberry.com/en/blackberry-uem/current/administration/adr1374514829642.html)

Assign a profile or IT policy to a user account

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. In the **IT policy and profiles** section, click +.
5. Click **IT policy** or a profile type.
6. In the drop-down list, click the name of the profile or IT policy that you want to assign to the user.
7. For IT policies and ranked profile types, if the profile type that you selected in step 5 is already assigned directly to the user, click **Replace**. Otherwise, click **Assign**.

(Source: http://help.blackberry.com/en/blackberry-uem/current/administration/ake1371676480571.html)

Device activation

When you activate a device, you associate the device with BlackBerry UEM so that you can manage devices and users can access work data on their devices.

When a device is activated, you can send IT policies and profiles to control the available features and manage the security of work data. You can also assign apps for the user to install. Depending on how much control the selected activation type allows, you may also be able to protect the device by restricting access to certain data, remotely setting passwords, locking the device, or deleting data.

You can assign activation types to accommodate the requirements of devices owned by your organization and devices owned by users. Different activation types give you different degrees of control over the work and personal data on devices, ranging from full control over all data to specific control over work data only.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/administration/activating_devices.html)

- *[f] authorizing control and access to the at least one multimedia source;*

Once a device has been activated with BlackBerry UEM, the system recognizes the device profile that has been created by the administrator. For example, the device profile directs what productivity apps the device has been assigned, the degree of protection based on the user's role and assigns IT policies and profiles to make sure the appropriate features are available to the mobile device. The system authorizes control and access to the multimedia source such as a corporate intranet or other multimedia content repository. Examples of multimedia content identified by the '575 patent include "image media such as GIF, JPEG and PNG; audio media such as Real Audio, wav, au; and video files such as QuickTime, MPEG, and Motion JPEG." ('575, col. 9:36-41.)

Flexible, Extensible, and Ready to Evolve

To better enable your organization, BlackBerry UEM integrates with many of the most common enterprise IT solutions. In addition to connecting with your Microsoft Active Directory or LDAP directory, it can manage access for Exchange ActiveSync (including Microsoft Office 365), integrate with your organization's PKI infrastructure, or restrict access to network resources through integration with Cisco ISE. As your needs evolve, you can also manage further BlackBerry capabilities to support enhanced collaboration, custom app development, identity and access management (IAM), or digital rights management (DRM) for secure file sharing.

(Source: https://us.blackberry.com/content/dam/blackberry-com/PDF/enterprise/ds-blackberry-uem.pdf)

Creating activation profiles

You can control how devices are activated and managed using activation profiles. An activation profile specifies how many and what types of devices a user can activate and the type of activation to use for each device type.

The activation type allows you to configure how much control you have over activated devices. You might want complete control over a device that you issue to a user. You might want to make sure that you have no control over the personal data on a device that a user owns and brings to work.

The assigned activation profile applies only to devices the user activates after you assign the profile. Devices that are already activated are not automatically updated to match the new or updated activation profile.

When you add a user to BlackBerry UEM, the Default activation profile is assigned to the user account. You can change the Default activation profile to suit your requirements, or you can create a custom activation profile and assign it to users or user groups.

Activation profiles do not apply to BlackBerry OS (version 5.0 to 7.1) devices.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/administration/activation-profile.html)

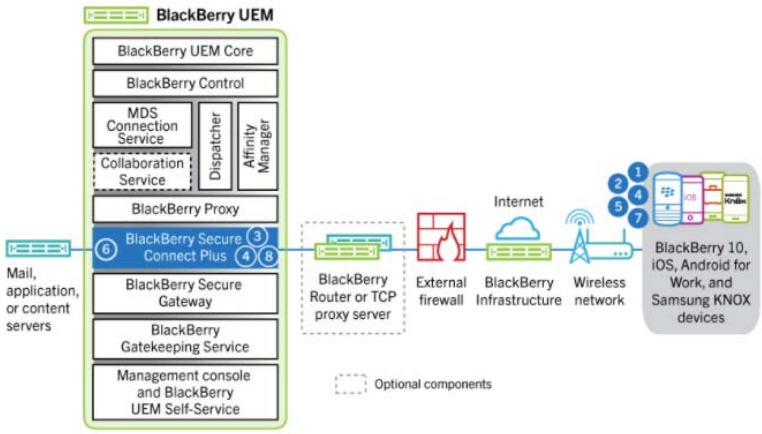
Device activation

When you activate a device, you associate the device with BlackBerry UEM so that you can manage devices and users can access work data on their devices.

When a device is activated, you can send IT policies and profiles to control the available features and manage the security of work data. You can also assign apps for the user to install. Depending on how much control the selected activation type allows, you may also be able to protect the device by restricting access to certain data, remotely setting passwords, locking the device, or deleting data.

You can assign activation types to accommodate the requirements of devices owned by your organization and devices owned by users. Different activation types give you different degrees of control over the work and personal data on devices, ranging from full control over all data to specific control over work data only.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/administration/activating_devices.html)



4. The device and BlackBerry Secure Connect Plus negotiate the tunnel parameters and establish a secure tunnel for the device through the BlackBerry Infrastructure. The tunnel is authenticated and encrypted end-to-end with DTLS.

5. The app uses the tunnel to connect to the application or content server using standard IPv4 protocols (TCP and UDP).

(Source: http://help.blackberry.com/en/blackberry-uem/current/architecture/lsh1428958213732.html)

- *[g] obtaining a mobile device transmission profile;*

Once a device has been activated with BlackBerry UEM, the system recognizes the device profile and user account that has been created by the administrator. The device profile includes work connection functionality, which defines how devices connect to work resources, such as content servers, for data transfer. On information and belief, in order to transmit data, the system obtains a mobile device transmission profile (e.g., information that describes the protocol of the wireless channel environment), such as data describing the Wi-Fi and/or application transmission protocols used in order to transmit data.

Wi-Fi, VPN, BlackBerry Secure Connect Plus, and other work connections

You can use profiles to set up and manage work connections for devices in your organization. Work connections define how devices connect to work resources in your organization's environment, such as mail servers, proxy servers, Wi-Fi networks, and VPNs. You can specify settings for BlackBerry 10, iOS, macOS, Android, and Windows devices in the same profile and then assign the profile to user accounts, user groups, or device groups.

(Source: http://help.blackberry.com/en/blackberry-uem/current/administration/wnw1513879285859.html)

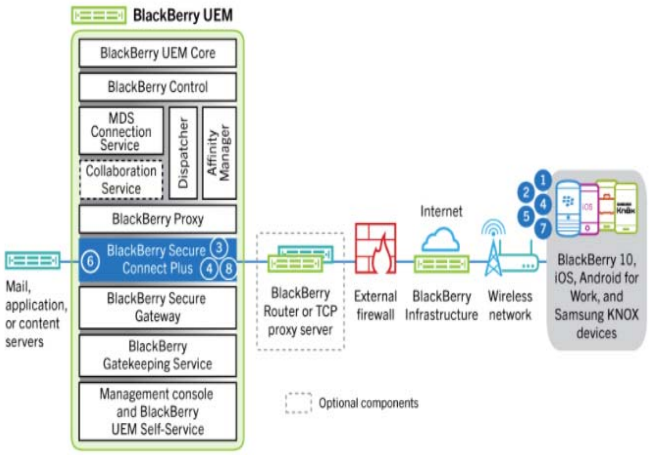
Sending and receiving work data

When devices that are active on BlackBerry UEM send and receive work data, they connect to your organization's mail, application, or content servers. For example, when they use the work email or calendar apps, devices establish a connection to your organization's mail server. When they use the work browser to navigate the intranet, devices establish a connection to the web server in your organization, and so on.

Depending on the type of device, the activation type, license types, and configuration settings, a device may establish connections to your organization's servers using the following paths:

Data Path	Description
Work Wi-Fi network	You can use BlackBerry UEM to configure Wi-Fi profiles for devices so that devices can connect to your organization's resources using your work Wi-Fi network.
VPN	You can use BlackBerry UEM to configure VPN profiles for devices or users may configure VPN profiles on their devices so that devices can connect to your organization's resources using a VPN.

(Source: http://help.blackberry.com/en/blackberry-uem/current/architecture/car1398183904582.html)



4. The device and BlackBerry Secure Connect Plus negotiate the tunnel parameters and establish a secure tunnel for the device through the BlackBerry Infrastructure. The tunnel is authenticated and encrypted end-to-end with DTLS.

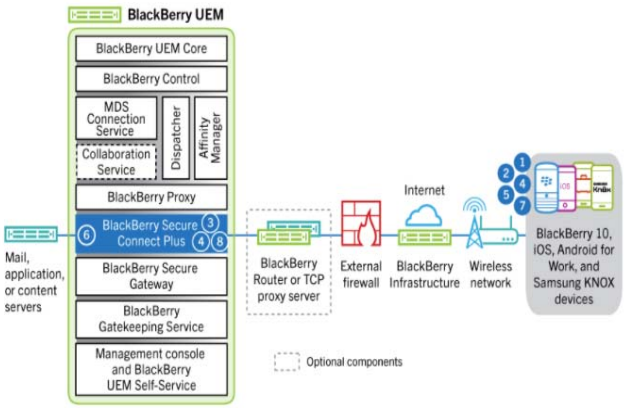
5. The app uses the tunnel to connect to the application or content server using standard IPv4 protocols (TCP and UDP).

(Source: http://help.blackberry.com/en/blackberry-uem/current/architecture/lsh1428958213732.html)

- *[h] providing a control channel from the mobile service platform to at least one multimedia server;*

BlackBerry UEM, including implementation with Secure Connect Plus, has functionality that communicates with devices to create a secure tunnel for data transfer from the device to the app. For example, BSCP signaling includes both a TLS tunnel and a DTLS tunnel with transcoder as illustrated below.

Data flow: Accessing an application or content server using BlackBerry Secure Connect Plus



4. The device and BlackBerry Secure Connect Plus negotiate the tunnel parameters and establish a secure tunnel for the device through the BlackBerry Infrastructure. The tunnel is authenticated and encrypted end-to-end with DTLS.

5. The app uses the tunnel to connect to the application or content server using standard IPv4 protocols (TCP and UDP).

(Source: http://help.blackberry.com/en/blackberry-uem/current/architecture/lsh1428958213732.html)

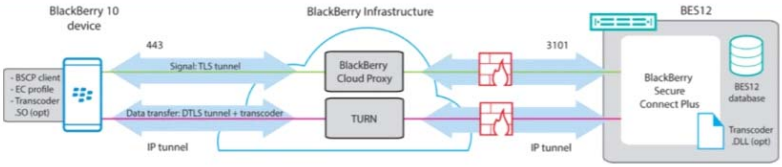


Figure 2 – BSCP signalling

Let's have a look at the signaling. Once the BES12 and the device have determined that BSCP is the best available connection method, meaning that no corporate Wi-Fi or BES12 VPN profile are available, then the device will send a request via a TLS connection through the BlackBerry Infrastructure that an IP tunnel should be established. BES12 receives this request through it's connection to the BlackBerry Infrastructure on port 3101.

After the request has been received the device and BES12 use the TURN protocol to negotiate the tunnel parameters. For the communication one tunnel is established and use for all the apps from within the work perimeter to the Enterprise resources.

(Source: http://devblog.blackberry.com/2015/07/bes12-v12-2-and-the-blackberry-secure-connect-plus-transport/)

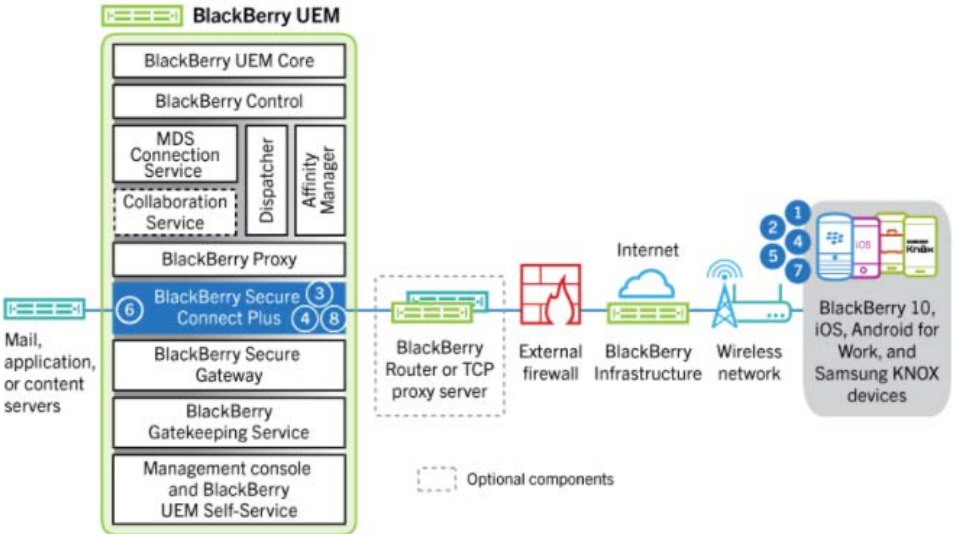
- *[i] providing multimedia data delivery information to the at least one multimedia server; and*

Multimedia data delivery information is provided to the multimedia server. For example, transmission-related data passes through BlackBerry UEM and its

components.

BlackBerry Infrastructure	The BlackBerry Infrastructure registers user information for device activation, validates licensing information for BlackBerry UEM, and provides a trusted path between the organization and every user based on strong, cryptographic, mutual authentication. BlackBerry UEM maintains a constant connection to the BlackBerry Infrastructure, meaning that organizations require only a single outbound connection to a trusted IP address to send data to users. All the data that travels between the BlackBerry Infrastructure and BlackBerry UEM is authenticated and encrypted to provide a secure communication channel into your organization for devices outside the firewall.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/architecture/ake1452094272560.html)



3. BlackBerry Secure Connect Plus receives the request from the BlackBerry Infrastructure through port 3101.
4. The device and BlackBerry Secure Connect Plus negotiate the tunnel parameters and establish a secure tunnel for the device through the BlackBerry Infrastructure. The tunnel is authenticated and encrypted end-to-end with DTLS.
5. The app uses the tunnel to connect to the application or content server using standard IPv4 protocols (TCP and UDP).
6. BlackBerry Secure Connect Plus transfers the IP data to and from your organization's network. BlackBerry Secure Connect Plus encrypts and decrypts traffic using FIPS-140 certified Certicom libraries.
7. The app receives and displays the data on the device.

(Source: http://help.blackberry.com/en/blackberry-uem/current/architecture/lsh1428958213732.html)

- *[j] providing multimedia data to the mobile device in response to the request via the at least one multimedia server.*

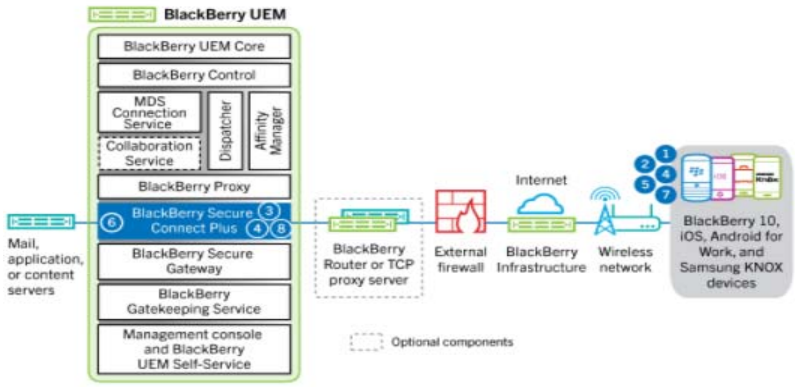
BlackBerry UEM responds to a request from a mobile device, creates a secure connection for data transfer, connects to third-party apps, and transmits data through BlackBerry UEM, and the data is then delivered to the end-user's mobile device. BlackBerry UEM provides the multimedia data to the mobile device, serving as an intermediary between the multimedia server and the mobile device.

6. BlackBerry Secure Connect Plus transfers the IP data to and from your organization's network. BlackBerry Secure Connect Plus encrypts and decrypts traffic using FIPS-140 certified Certicom libraries.

7. The app receives and displays the data on the device.

8. As long as the tunnel is open, supported apps use it to access network resources. When the tunnel is no longer the best available method to connect to your organization's network, BlackBerry Secure Connect Plus terminates it.

(Source: http://help.blackberry.com/en/blackberry-uem/current/architecture/lsh1428958213732.html)



1. The user opens an app to access work data from a content or application server behind your organization's firewall.
   - For BlackBerry 10 devices and Android devices with a work profile, all work space apps use BlackBerry Secure Connect Plus.
   - For iOS devices, you specify whether all apps or only specified apps use BlackBerry Secure Connect Plus.
   - For Android devices with a work profile, all work space apps except those you choose to restrict use BlackBerry Secure Connect Plus.
   - For Samsung KNOX Workspace devices, you specify whether all work space apps or only specified work apps use BlackBerry Secure Connect Plus.
2. The device sends a requests through a TLS tunnel, over port 443, to the BlackBerry Infrastructure to request a secure tunnel to the work network. The signal is encrypted by default using FIPS-140 certified Certicom libraries. The signaling tunnel is encrypted end-to-end.
3. BlackBerry Secure Connect Plus receives the request from the BlackBerry Infrastructure through port 3101.
4. The device and BlackBerry Secure Connect Plus negotiate the tunnel parameters and establish a secure tunnel for the device through the BlackBerry Infrastructure. The tunnel is authenticated and encrypted end-to-end with DTLS.
5. The app uses the tunnel to connect to the application or content server using standard IPv4 protocols (TCP and UDP).
6. BlackBerry Secure Connect Plus transfers the IP data to and from your organization's network. BlackBerry Secure Connect Plus encrypts and decrypts traffic using FIPS-140 certified Certicom libraries.
7. The app receives and displays the data on the device.
8. As long as the tunnel is open, supported apps use it to access network resources. When the tunnel is no longer the best available method to connect to your organization's network, BlackBerry Secure Connect Plus terminates it.

(Source: http://help.blackberry.com/en/blackberry-uem/current/architecture/lsh1428958213732.html)

BlackBerry Infrastructure	The BlackBerry Infrastructure registers user information for device activation, validates licensing information for BlackBerry UEM, and provides a trusted path between the organization and every user based on strong, cryptographic, mutual authentication. BlackBerry UEM maintains a constant connection to the BlackBerry Infrastructure, meaning that organizations require only a single outbound connection to a trusted IP address to send data to users. All the data that travels between the BlackBerry Infrastructure and BlackBerry UEM is authenticated and encrypted to provide a secure communication channel into your organization for devices outside the firewall.

(Source: http://help.blackberry.com/en/blackberry-uem/12.7/architecture/ake1452094272560.html)

- *3. The method of claim 1 further comprising providing a user control path from the mobile device to the at least one controllable multimedia source via the at least one multimedia server for controlling the at least controllable multimedia source from the mobile device.*

BlackBerry UEM provides a user control path from the mobile device to the at least one controllable multimedia source via the at least one multimedia server for controlling the at least controllable multimedia source from the mobile device, as discussed above with respect to Claim 1. UEM provides a path for a user of a mobile device, such as a smartphone, connected to a multimedia source, such as a corporate intranet, to control the multimedia source from the mobile device.

- *4. The method of claim 1 further comprising providing a user control path from the mobile device to the at least one controllable multimedia source via the mobile service platform for controlling the at least controllable multimedia source from the mobile device.*

BlackBerry UEM provides a user control path from the mobile device to the at least one controllable multimedia source via the mobile service platform for controlling the at least controllable multimedia source from the mobile device, as discussed above with respect to Claim 1. UEM provides a path for a user of a mobile device, such as a

smartphone, connected to a multimedia source, such as a corporate intranet, to control the multimedia source from the mobile device.

- *22. The method of claim 1 wherein the mobile device includes devices selected from the group consisting of SMS mobile phones, WAP mobile phones, PDA devices, Instant Messaging devices, e-mail devices, two way pagers, pocket PCs, handheld PCs, and smart phones.*

BlackBerry UEM can connect to a host of devices, including mobile phones, laptops, and even wearable headsets. BlackBerry's UEM helps "[s]ecure and manage mobile devices, laptops and other endpoints across different operating systems and ownership models. Control user access to business apps, data and content. And do it all from a single, easy-to-use management console, with an extensive set of policies and profiles to suit your needs."

(Source: https://us.blackberry.com/content/dam/blackberry-com/PDF/enterprise/ds-blackberry-uem.pdf)

Key BlackBerry UEM features

Feature	Description
Multiplatform device management	You can manage iOS, macOS, Android, Windows, and BlackBerry devices.

(Source: http://help.blackberry.com/en/blackberry-uem/current/overview-and-whats-new/dsc1395171862872.html)

47. Facebook is entitled to relief as a result of BlackBerry's infringement, including without limitation monetary damages no less than a reasonable royalty.

COUNT III: INFRINGEMENT OF U.S. PATENT NO. 6,356,841

48. Facebook incorporates by reference and re-alleges all foregoing paragraphs of this Complaint as if fully set forth herein.

49. Facebook is the owner by assignment of U.S. Patent No. 6,356,841

("'841 patent"), entitled "G.P.S. management system," including the exclusive right to bring suit to enforce the patent and the exclusive right to obtain relief for infringement. The '841 patent was duly and legally issued by the U.S. Patent and Trademark Office on March 12, 2002. The patent is based on U.S. Patent Application Ser. No. 09/474,368 filed on December 29, 1999.

50. A true and correct copy of the '841 patent is attached as Exhibit C.

51. The '841 patent is valid and enforceable under the United States Patent Laws.

SUMMARY OF INVENTION

52. The '841 patent originated with BellSouth Intellectual Property Corporation, as indicated on the face of the patent. BellSouth Intellectual Property Corporation was affiliated with telecommunications provider BellSouth Corp., which traced its roots to the AT&T corporate family. BellSouth Corp. was acquired by AT&T Inc. in 2006 for a reported $85.8 billion.

53. The '841 patent notes that Global Positioning System (GPS) data was known and used prior to the patented invention, but its use was limited and subject to a number of drawbacks. As stated in the patent: "One of the drawbacks of conventional G.P.S. systems is the local and isolated nature of the G.P.S. information. Currently, the position information is only sent to the local user and the location history, or where the user has been, cannot be determined. Furthermore, conventional G.P.S. systems do not allow centralized storage and processing of information and conventional G.P.S. systems cannot track multiple G.P.S. users." ('841, col. 1:17-24.)

54. The invention of the '841 patent provides centralized tracking and analysis from a "central location," enabling one or more remote devices and their associated items, such as vehicles, to be tracked centrally. The patent states: "The invention generally allows accurate and convenient tracking and management of multiple G.P.S.-equipped remote entities." ('841, col. 2:55-57.) The inventive system reflected in the patent also includes numerous additional features that provide benefits as described in

the specification. For example, "the system includes provisions that allow information stored in the remote unit to be transmitted to the central location during periods of relative inactivity. This feature allows information to be transferred from the remote unit to the central location without interfering with the function of the system during busy or active periods of time." (*Id.*, col. 1:61-67.)

55. The invention also provides additional benefits such as a power-saving state to conserve power usage by the remote GPS-equipped device. The patent includes a section entitled "Power Conservation Features" that states as follows:

> The invention includes provisions to conserve power. When the system detects an ignition off condition, the system processes all of the computing steps associated with the detection of an ignition off condition, and then the ICU enters a 'sleep' mode in order to reduce power consumption. When in sleep mode, power shall be supplied only to those components that must still function when the vehicle is not moving.
>
> During the "sleep mode" the alert call features, including the RAT (Remote Alert Transmitter) button, still function. The preferred way the system allows the alert call feature to function during a state of 'sleep,' such that the system comes out of sleep mode when the system senses an activation of a technician alert call, either from an in-vehicle button or a remote button, and the ICU comes out of the sleep mode long enough to perform alert call processing functions.
>
> System parameters, location of the vehicle, and other stored data is maintained while the ICU is in sleep mode. Turning the vehicle ignition on causes the ICU to come out of the sleep mode and resume normal processing.
>
> Preferably, the ICU is designed to conserve power during all of its operating modes. Primary vehicle power consumption by all G.P.S. components within the vehicle should not to exceed 1 Amp hour for any twenty-four hour period.

('841, col. 11:45-12:2.)

56. The claims of the '841 patent, including the claims infringed by BlackBerry, reflect the technological benefits and advantages over the prior art that the specification describes. For example, claims 12 and 26 recite that a remote unit receiving GPS information has a first state where it consumes a first quantity of power and a second state where it consumes a second quantity of power. These claim features reflect the specification's teachings that the invention includes provisions to conserve power, such as a "sleep" mode and related functionality to reduce power consumption. Claim 12 further recites that where the remote unit stores the GPS information in a memory and transmits the GPS information to a central location when the unit is in a second state, and claims 19 and 25 recite that the remote unit detects a loss of GPS signal and stores information associated with the loss of signal, reflecting the data storage-related features of the invention as described in the specification.

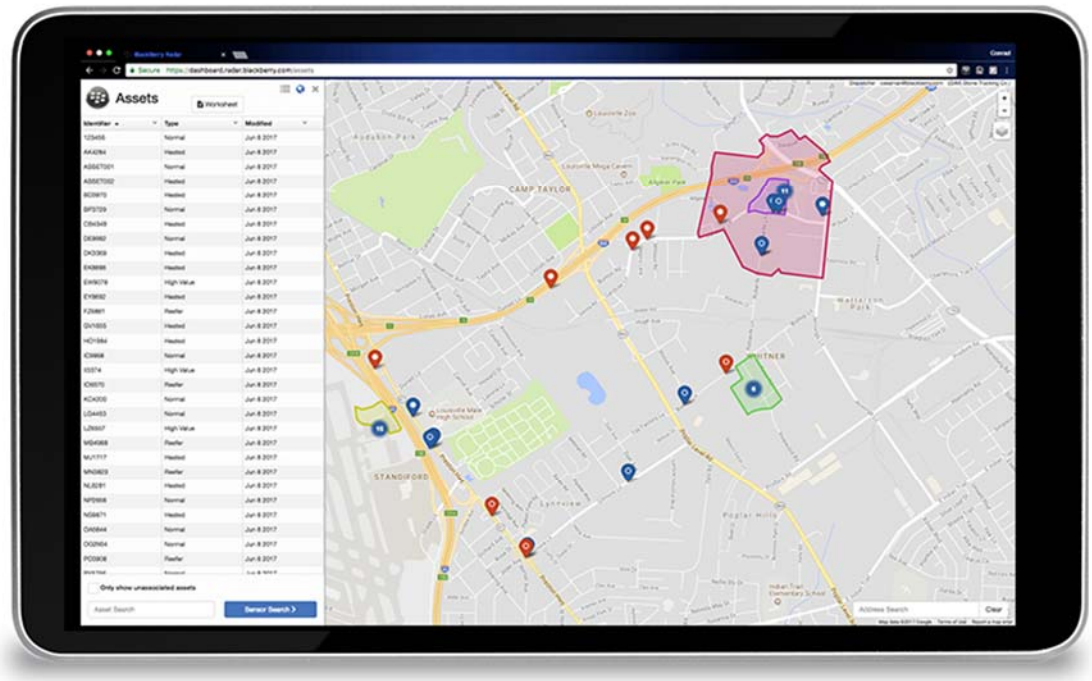
BLACKBERRY'S INFRINGEMENT

57. BlackBerry has infringed and is continuing to infringe the '841 patent by making, using, selling and/or offering to sell in the United States, or importing into the United States, products or processes that practice the '841 patent in violation of 35 U.S.C. § 271(a), including without limitation BlackBerry's Radar products, including Radar-L and Radar-M, and related software products and system functionality.

58. BlackBerry's infringement of the '841 patent has caused and will continue to cause damage for which Facebook is entitled to recovery under 35 U.S.C. § 284.

59. As set forth below, BlackBerry infringes the '841 patent. The following description is exemplary and illustrative of BlackBerry's infringement based on publicly available information. Facebook expects to further develop the evidence of BlackBerry's infringement after obtaining discovery from BlackBerry in the course of this action.

60. BlackBerry's Radar products provide asset tracking and monitoring functionality. Using web-based software, customers can view the locations of assets, such as trucks in a fleet, which have Radar devices installed. An illustration by BlackBerry of the Radar Dashboard user interface is provided below.



(Source: https://us.blackberry.com/qnx-radar/trailer-chassis-and-container-tracking/radar-solution/radar-services)

61. Illustrative figures from the '841 patent are provided below.

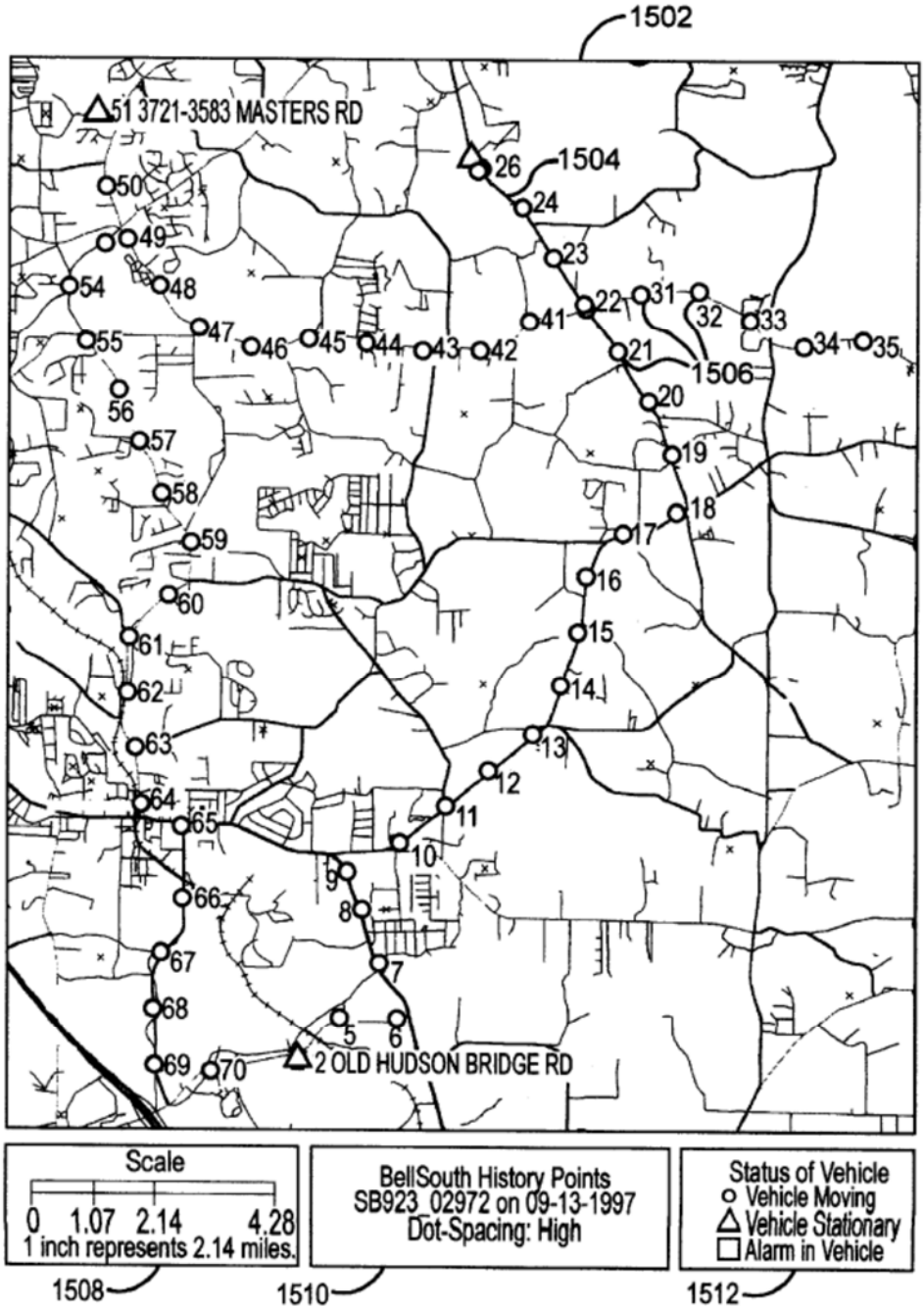

1502
51 3721-3583 MASTERS RD
1504
1506
2 OLD HUDSON BRIDGE RD
Scale
0 1.07 2.14 4.28
1 inch represents 2.14 miles.
1508
BellSouth History Points
SB923_02972 on 09-13-1997
Dot-Spacing: High
1510
Status of Vehicle
Vehicle Moving
Vehicle Stationary
Alarm in Vehicle
1512

FIG.15

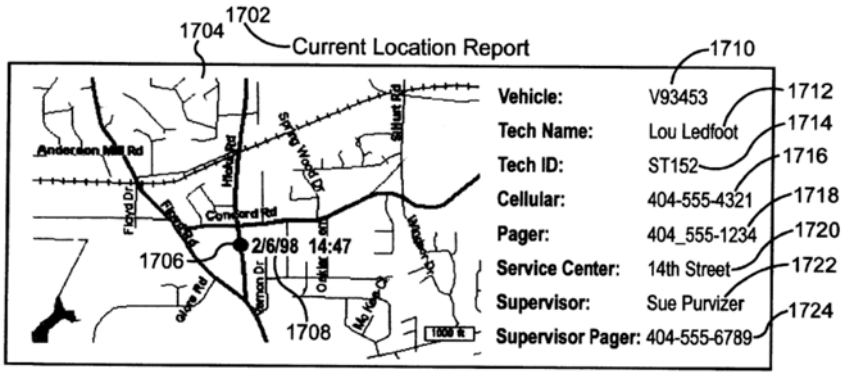


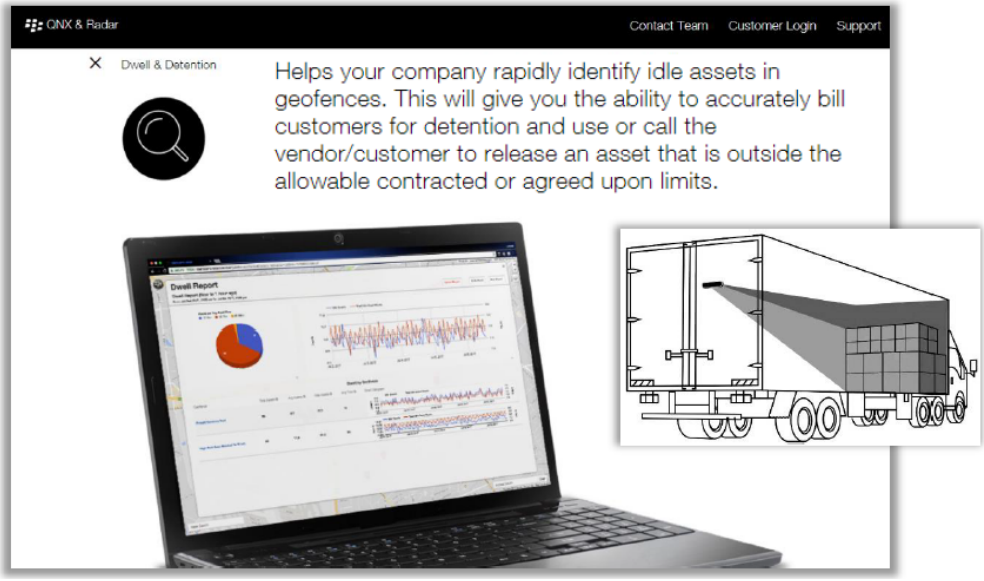
FIG.17

('841, Figs. 15 and 17.)

62. An illustrative description of BlackBerry's infringement on an element-by-element basis is provided below for exemplary claims of the patent.

- *12[p]. A system comprising:*

BlackBerry's Radar products including associated software comprise an asset tracking system. The Radar device contains sensors and attaches to commercial vehicles and reports various vehicle conditions including location, motion, humidity, and door events. The reports can be provided to a central location, such as to monitor a truck fleet that has Radar devices installed.



> Helps your company rapidly identify idle assets in geofences. This will give you the ability to accurately bill customers for detention and use or call the vendor/customer to release an asset that is outside the allowable contracted or agreed upon limits.

(Source: https://us.blackberry.com/qnx-radar/trailer-chassis-and-container-tracking/radar-solution/radar-services)

- *12[a] (a) a central location;*

As shown above, the Radar system includes a central location, such as a location from which the Radar devices and associated assets are monitored. BlackBerry states that it provides "securely hosted cloud services" for Radar. (Source: https://docs.radar.blackberry.com/.) BlackBerry directs users to access a Dashboard interface through the web at https://dashboard.radar.blackberry.com/.

- *12[b] (b) a remote unit in communication with the central location, the remote unit in communication with a Global Positioning System receiver and receiving Global Positioning System information from the Global Positioning System receiver; wherein*

The BlackBerry Radar-L and Radar-M asset tracker devices each contain components including sensor and processing components and a GPS receiver. Each device contains components that communicate with the central location such as by transmitting location and sensor data.

Radar-L

Technical Specifications

Communications
UMTS: Bands 1, 2, 5, 6, 8 HSDPA cat 8, HSUPA cat 6
- 800/850/900/1900/2100 MHz

GSM/EDGE Bands 2, 3, 5, 8 multi-slot class 12
- 850/900/1800/1900 MHz

Location
GPS / GLONASS

Sensors
Sensors for movement and door opening and closing detection

Battery
High Capacity Non-Rechargeable Battery operating at 10.8V

Physical
Single box construction with removable battery
- 173mm X 117mm X 52mm thick (6.8" X 4.6" X 2.0")
- Weight: 700g (25oz.)

Radar-M

Technical Specifications

Communications
UMTS: Bands 1, 2, 5, 6, 8 HSDPA cat 8, HSUPA cat 6
- 800/850/900/1900/2100 MHz

GSM/EDGE Bands 2, 3, 5, 8 multi-slot class 12
- 850/900/1800/1900 MHz

Location
GPS / GLONASS

Sensors
- Sensors hub for movement and door opening and closing detection
- Temperature, pressure and humidity sensors to monitor the conditions inside the container
- Cargo load sensor to determine load status of container

Battery
High Capacity Non Rechargeable Primary Battery operating at 7.2V

Physical
Two pieces solution with battery and sensors inside and external module with the antenna and radios
- **Inside:** 290mm X 96mm X 53mm thick (11 27/64" x 3 25/32" x 2 3/32" thick)
- **Outside:** 290mm X 96mm X 28mm thick (11 27/64" x 3 25/32" x 1 7/64" thick)
- **Weight:** 1.3kg (2.9 lbs)

- *12[c] the remote unit having a first state wherein the remote unit consumes a first quantity of power and a second state where the remote unit consumes a second quantity of power, the first quantity of being greater than the second quantity of power;*

The remote unit has multiple different states that consume different quantities of power. For example, when a Radar device has a low battery and/or detects a low temperature and is not in continuous motion, the data update rate will be decreased (for example, decreasing the data update rate from the default 15 minutes to 30 minutes or more) "to maintain battery life." By decreasing the data update rate, the device consumes less power and therefore maintains battery life.

Low temperature or low battery conditions

On a Radar module, in low battery or low temperature (temperature <= -10 degrees Celsius/14 degrees Fahrenheit) conditions, the system will decrease the data update frequency to maintain battery life, overriding the default update rate with a lower rate.

The sections below detail the conditions and the update rates under those conditions.

Note that update frequency changes only affect when GPS information and sensor information are uploaded to the Radar cloud. While an asset is in continuous motion, GPS information is collected every five minutes, regardless of the update frequency setting.

Low battery

When low battery is detected, the asset data update rate will be increased from the default 15 minutes to 30 minutes.

Low temperature

When the battery is OK and the temperature is detected to be equal to or lower than -10 degrees Celsius (14 degrees Fahrenheit), the data update rate will be decreased based on the temperature reading, as detailed in the table below.

Temperature	Update Frequency
<= -10 degrees Celsius/14 degrees Fahrenheit	30 minutes
<= -20 degrees Celsius/-4 degrees Fahrenheit	1 hour
<= -30 degrees Celsius/-22 degrees Fahrenheit	2 hours
<= -40 degrees Celsius/-40 degrees Fahrenheit	3 hours

Note: As the temperature changes, the update frequency will be adjusted accordingly.

Low battery and low temperature

In the case of both low battery *and* low temperature, the data update rate will be further decreased based on the temperature reading, as detailed in the table below.

Temperature and Other Conditions	Update Frequency
<= -10 degrees Celsius/14 degrees Fahrenheit	1 hour
<= -20 degrees Celsius/-4 degrees Fahrenheit	3 hours
<= -30 degrees Celsius/-22 degrees Fahrenheit	6 hours
<= -40 degrees Celsius/-40 degrees Fahrenheit	12 hours
<= -18 degrees Celsius/-0.4 degree Fahrenheit, battery overload detected, such as from low battery, extended use, and/or extreme cold	24 hours

Note: As the temperature or battery condition changes, the update frequency will be adjusted accordingly.

(Source: https://docs.radar.blackberry.com/guides/user_guide_asset/#low-temperature-or-low-battery-conditions)

- *12[d] the remote unit storing the Global Positioning System information in a memory wherein the remote unit transmits the Global Positioning System information to the central location when the remote unit is in the second state.*

The remote unit stores GPS data in a memory. For example, in normal operation, a Radar device takes data readings every 5 minutes and uploads data to the network every 15 minutes, confirming that the device stores the data in a memory.

In the second state of operation (lower-power state with low battery and/or low

temperature), the device also transmits GPS data to the central location at a different rate, as indicated by the evidence cited for Claim 12[c] above.

Frequent Updates
Data readings are taken every five minutes and uploaded at 15-minute intervals

Sophisticated sensors for cargo tracking
Comprehensive data is collected every 5 minutes by BlackBerry Radar's state-of-the-art sensors. Based on this data, you can provide your customers with detailed reports, demonstrating the prescribed conditions under which their product has been delivered. In addition, you can receive instant alerts when sensor data is outside the prescribed parameters.

(Source: https://www.fleetcomplete.com/en/products/blackberry-radar/)

- *15. The system according to claim 12, wherein other information, in addition to the Global Positioning System information, is stored in the memory.*

On information and belief, Radar device memories store GPS data as well as other information such as sensor data, as indicated for Claim 12[d]. As noted for Claim 12[d], in normal operation the device takes data readings every 5 minutes and uploads data every 15 minutes, storing data in the interim.

- *16. The system according to claim 12, wherein other information is stored in the memory.*

See claim 15.

- *23[p]. A system comprising:*

See claim 12[p].

- *23[a]. a remote unit in communication with a central location, the remote unit comprising a Global Positioning System receiver, a processor in communication with the Global Positioning System receiver and in communication with a memory,*

The BlackBerry Radar-L and Radar-M asset tracker devices each contain components including a GPS receiver, processor, and memory. Both the Radar-L and

Radar-M models also contain cellular communication technology used to transmit location and sensor data back to a central location. The devices contain memory as indicated by the fact that they record sensor data every 5 minutes and upload the data every 15 minutes in normal operation.

Radar-L

Technical Specifications

Communications
UMTS: Bands 1, 2, 5, 6, 8 HSDPA cat 8, HSUPA cat 6
- 800/850/900/1900/2100 MHz

GSM/EDGE Bands 2, 3, 5, 8 multi-slot class 12
- 850/900/1800/1900 MHz

Location
GPS / GLONASS

Sensors
Sensors for movement and door opening and closing detection

Battery
High Capacity Non-Rechargeable Battery operating at 10.8V

Physical
Single box construction with removable battery
- 173mm X 117mm X 52mm thick (6.8" X 4.6" X 2.0")
- Weight: 700g (25oz.)

Radar-M

Technical Specifications

Communications
UMTS: Bands 1, 2, 5, 6, 8 HSDPA cat 8, HSUPA cat 6
- 800/850/900/1900/2100 MHz

GSM/EDGE Bands 2, 3, 5, 8 multi-slot class 12
- 850/900/1800/1900 MHz

Location
GPS / GLONASS

Sensors
- Sensors hub for movement and door opening and closing detection
- Temperature, pressure and humidity sensors to monitor the conditions inside the container
- Cargo load sensor to determine load status of container

Battery
High Capacity Non Rechargeable Primary Battery operating at 7.2V

Physical
Two pieces solution with battery and sensors inside and external module with the antenna and radios
- **Inside:** 290mm X 96mm X 53mm thick (11 27/64" x 3 25/32" x 2 3/32" thick)
- **Outside:** 290mm X 96mm X 28mm thick (11 27/64" x 3 25/32" x 1 7/64" thick)
- **Weight:** 1.3kg (2.9 lbs)

- *23[b]. the remote unit transmitting Global Positioning System data to the central location,*

Using their cellular transceivers, the Radar-M and Radar-L transmit GPS location data to the BlackBerry cloud.

Data-driven Business Intelligence

Three device sensors that allow for event-driven alerts

Location:
Track assets when in motion or stationary and with customized geofencing. Drivers can find fleet assets using their mobile phones.

Motion Detection:
Know when your asset is on the move or in/out of a geofence.

Doors Events:
Monitor open/close status when mounted on doors.

Powerful Interactive Reports and Alerts

The Radar-M cloud-based platform presents the user with simple-to-understand and powerful interactive reports designed specifically for managing mobile transportation assets.

Users can receive event-driven alerts that can be triggered by the sensor data or activity within geofences.

- *23[c]. wherein the central location compares the Global Positioning System data to a predetermined parameter having a range of acceptable values, and notes if the predetermined parameter is outside the range of acceptable values; and*

The central location processes the location data in comparison with stored parameter data, such as to determine whether an asset is inside or outside of a geofence and provide event-driven alerts to customers. The BlackBerry Radar web interface can display a map with geofences and asset locations. There is also a tab that displays asset events. The system receives GPS data to determine if the vehicle location is inside or outside of "acceptable values" associated with the geofence.

View geofence information

A geofence is a virtual region created on a map to represent an actual geographic area. Geofences are used to define areas for which certain types of asset tracking data need to be collected, for example, a distribution center where cargo is loaded and unloaded.

1. Open the **Geofences** view to see the list of geofences.
2. Click on any geofence. This opens the geofence view and locates the geofence on the map.
   - On the map, you can double click the geofence to zoom in.
   - On the geofence view, you can see
     - Which asset reports are included in this geofence (the "Include..." checkboxes)
     - What alerts are set for each asset type

Note: Only an administrator can modify geofences and their settings.

Geofence alerts	• Enter: Asset has entered the specified geofence. • Exit: Asset has left the specified geofence.

(Source: https://docs.radar.blackberry.com/guides/user_guide_otherinfo/)

- *23[d]. wherein the length of time the remote unit remains in a stationary position is monitored and is compared to a predetermined stationary time, and if the length of time that the remote unit remains in a stationary position is greater than the predetermined stationary time, the system notes an exception.*

In addition to geofences, BlackBerry Radar Dwell Detection can identify idle assets that have remained in one location for too long. For example, according to

BlackBerry, if a truck remains at a customer location for too long, the trucking company may adjust the bill for that customer. Alternatively, an employer can track how long its drivers remain at a given location. As recited in Claim 23, Dwell Detection can be combined with geofencing to identify idle assets that remain within specified areas.

Dwell & Detention

Helps your company rapidly identify idle assets in geofences. This will give you the ability to accurately bill customers for detention and use or call the vendor/customer to release an asset that is outside the allowable contracted or agreed upon limits.

Automated Yard Check

Displays information on trailers located within customized geofences. Eliminates manual physical yard checks that are inaccurate. This reduces labor costs and wasted time, and gives you global visibility to all your yards at the touch of a button.

Fleet Utilization

Allows you to identify idle assets, optimize customer equipment pools and provide accurate information to operations teams for new equipment procurement or rentals. In combination with key performance indicators for your company, this report can help you track efficiency and increase profits.

(Source: https://us.blackberry.com/qnx-radar/trailer-chassis-and-container-tracking/radar-solution/radar-services)

Subscribe to alert notifications

When an asset detects an alert condition, an alert message is sent to its registered users through email. You can subscribe to receive alert notifications.

The conditions that trigger alert notifications are set in each asset type, but can also be overridden in individual assets or geofences. For more information about alerts, see Events and alerts.

Alerts

Alert	Description
Door alerts	• Open: Asset door is open. • Closed: Open: Asset door is closed.
Movement alerts	• Start moving: Asset has started moving. • Stop moving: Asset has stopped moving. • Extended Stop: Asset stop time has exceeded the time set for extended stopover

(Source: https://docs.radar.blackberry.com/guides/user_guide_otherinfo/)

For example, the BlackBerry web interface can display a "Dwell Report" identifying assets that have remained stationary and/or within a geofence for an extended period of time.

(Source: https://us.blackberry.com/qnx-radar/trailer-chassis-and-container-tracking/radar-solution/radar-services)

- *25. The system according to claim 23, wherein the remote unit detects a loss of Global Positioning System signal and stores information associated with the loss of signal.*

On information and belief, when the Radar device detects a loss of GPS signal, the unit detects the loss of signal and stores information associated with the loss of signal.

- *26. The system according to claim 23, wherein the remote unit has a first state wherein the remote unit consumes a first quantity of power and a second state where the remote unit consumes a second quantity of power, the first quantity of power being greater than the second quantity of power.*

The Radar device has multiple different states that consume different quantities of power, as discussed above for Claim 12. For example, when the device has a low battery and/or detects a low temperature and the device is not in continuous motion, the data update rate will be decreased, which consumes less power.

Low temperature or low battery conditions

On a Radar module, in low battery or low temperature (temperature <= -10 degrees Celsius/14 degrees Fahrenheit) conditions, the system will decrease the data update frequency to maintain battery life, overriding the default update rate with a lower rate.

The sections below detail the conditions and the update rates under those conditions.

Note that update frequency changes only affect when GPS information and sensor information are uploaded to the Radar cloud. While an asset is in continuous motion, GPS information is collected every five minutes, regardless of the update frequency setting.

Low battery

When low battery is detected, the asset data update rate will be increased from the default 15 minutes to 30 minutes.

Low temperature

When the battery is OK and the temperature is detected to be equal to or lower than -10 degrees Celsius (14 degrees Fahrenheit), the data update rate will be decreased based on the temperature reading, as detailed in the table below.

Temperature	Update Frequency
<= -10 degrees Celsius/14 degrees Fahrenheit	30 minutes
<= -20 degrees Celsius/-4 degrees Fahrenheit	1 hour
<= -30 degrees Celsius/-22 degrees Fahrenheit	2 hours
<= -40 degrees Celsius/-40 degrees Fahrenheit	3 hours

Note: As the temperature changes, the update frequency will be adjusted accordingly.

Low battery and low temperature

In the case of both low battery *and* low temperature, the data update rate will be further decreased based on the temperature reading, as detailed in the table below.

Temperature and Other Conditions	Update Frequency
<= -10 degrees Celsius/14 degrees Fahrenheit	1 hour
<= -20 degrees Celsius/-4 degrees Fahrenheit	3 hours
<= -30 degrees Celsius/-22 degrees Fahrenheit	6 hours
<= -40 degrees Celsius/-40 degrees Fahrenheit	12 hours
<= -18 degrees Celsius/-0.4 degree Fahrenheit, battery overload detected, such as from low battery, extended use, and/or extreme cold	24 hours

Note: As the temperature or battery condition changes, the update frequency will be adjusted accordingly.

(Source: https://docs.radar.blackberry.com/guides/user_guide_asset/#low-temperature-or-low-battery-conditions)

- *27. The system according to claim 23, wherein at least one report is generated.*

The Radar system generates reports (as well as alert message reports) when assets are outside of a geofence or are in an extended idle state, as shown in the screenshots above for Claim 23.

- *28. The system according to claim 23, wherein the system notes if the predetermined parameter is outside the range of acceptable values by*

generating a report that includes information related to the instances where the predetermined parameter is outside the range of acceptable values.

The Radar system generates reports that identify and display (as well as alert message reports) when assets are outside of a geofence or are in an extended idle state, as shown in the screenshots above for Claim 23.

63. Facebook is entitled to relief as a result of BlackBerry's infringement, including without limitation monetary damages no less than a reasonable royalty.

COUNT IV: INFRINGEMENT OF U.S. PATENT NO. 7,228,432

64. Facebook incorporates by reference and re-alleges all foregoing paragraphs of this Complaint as if fully set forth herein.

65. Facebook is the owner by assignment of U.S. Patent No. 7,228,432 ("'432 patent"), entitled "Method and apparatus for providing security for a computer system," including the exclusive right to bring suit to enforce the patent and the exclusive right to obtain relief for infringement. The '432 patent was duly and legally issued by the U.S. Patent and Trademark Office on June 5, 2007. The patent is based on U.S. Patent Application Ser. No. 10/660,335 filed on September 11, 2003.

66. A true and correct copy of the '432 patent is attached as Exhibit D.

67. The '432 patent is valid and enforceable under the United States Patent Laws.

SUMMARY OF INVENTION

68. The '432 patent originated with the Hewlett Packard Company ("HP") corporate family. HP was a leading multinational technology company that was founded and headquartered in Palo Alto, California. HP was succeeded by corporate entities including publicly-traded HP Inc. and Hewlett Packard Enterprise.

69. The '432 patent acknowledges that computer networks existed that allowed files, programs, and other information to be transferred from one computer system to another system, including the use of security systems to prevent unauthorized

intrusions or attacks. ('432, col. 1:7-24.) However, prior art security functions suffered from drawbacks. For example, according to the patent, while computer viruses could be pre-classified to assist in identifying malicious code, computer systems could be left vulnerable "because a virus may be unknown or unclassified." (*Id.*, col. 1:28-29.) "As a result, the computer system is not able to remove an unknown virus before it attacks the computer system." (*Id.*, col. 1:29-31.) Computing performance impact was also an issue. For example, the patent explains that "the performance of the central processing unit ('CPU') may be impacted by the operation of security functions of the computer system. The computer system's overall performance may be diminished because the security functions are consuming the resources of the CPU." (*Id.*, col. 1:31-36.)

70. To address the perceived deficiencies in the prior art, the inventions taught by the '432 patent use a security processor to access and validate a requested file, which may then be provided to another processor. The patent explains how the disclosed invention provides an improved approach that may enhance the performance of a computer system:

> The disclosed embodiments provide an improved approach that may address one or more of the issues discussed above, while enhancing the performance of a computer system. With computer systems, security functions may be provided to protect the system. The security functions may be managed by a device or component, such as a processor, that is within the computer system or external to the computer system. In the disclosed embodiments, the security of the computer system is maintained in a manner that: (1) protects against defeat by thread models or technologies; (2) minimizes interaction with the CPU; and (3) allows trapping of code that is unknown or unclassified.

(*Id.*, col. 2:18-29.)

71. As one example taught by the '432 patent, the disclosed techniques "may enable a computer system to operate in a more efficient manner by having a security co-processor that protects against defeat by thread models or technologies." (*Id.*, col.

2:31-34.) The patent explains:

> By having a security co-processor examine code and activities that are independent of the operating system, the threaded programs are unable to defeat the security of the computer system. In addition, the security co-processor may minimize the performance impact on the central processing unit ("CPU") of a computer system by performing the security functions, which allows the CPU to devote more resources to non-security related functions. Furthermore, the security co-processor may examine new code without the code being pre-classified. Thus, as new viruses are introduced, the security co-processor may trap the unknown or unclassified code before the CPU is damaged by an attack from the code.

(*Id*., col. 2:37-49.)

72. In one illustrative example embodiment, a security co-processor (designated as item **111**) may examine code independent of the operating system of a computer system (item **100**) and a processor complex (item **102**) or other computers in a computer network. (*Id*., col. 4:11-35, Fig. 2.) Using this architecture, "the security co-processor **111** may enable the computer system **100** to prevent thread technologies and unknown code from attacking the computer system **100**. As a benefit to the computer system **100**, the security co-processor **111** may examine code independently of the processor complex **102**, which may be executing an operating system. As such, the security co-processor **111** may trap code that is unknown or unclassified to prevent it from impacting the performance or integrity of the computer system **100**." (*Id*., col. 4:13-17.) In addition, "[b]ecause the security co-processor **111** performs the security functions and activities, it frees the use of the CPU cycles on the processor complex **102** for other computing activities." (*Id*., col. 4:17-20.)

73. The claims of the '432 patent reflect the technological improvements taught by the specification. For example, each claim recites a security processor used to validate a file that is distinct from another processor. The architecture reflected in the

claims, including a security processor distinct from another processor, can be used to enhance the operation of the computer system or systems involved in the implementation, as described in the specification. For example, as the specification teaches, any malicious code can be isolated by the security processor so that it does not harm the performance or integrity of the other processor or associated operating system or computer system. Furthermore, as explained by the specification, the use of a security processor distinct from another processor also minimizes the performance impact on the other processor, allowing the other processor to devote resources to non-security related computing activities.

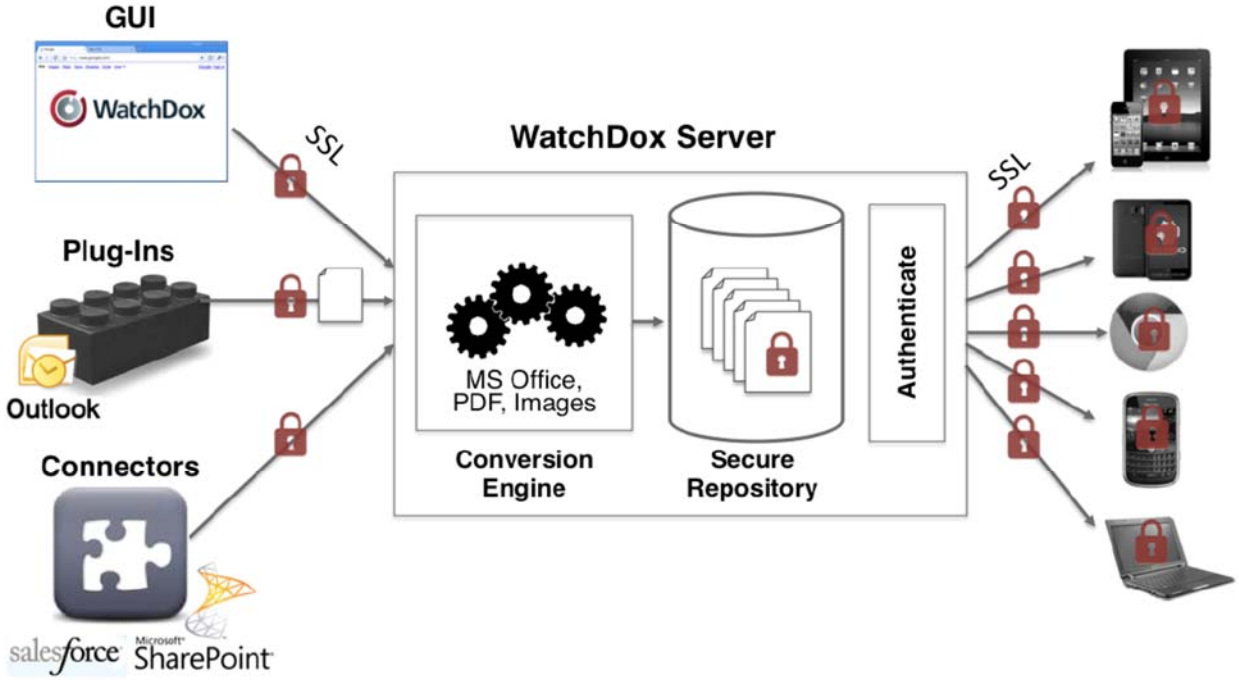
BLACKBERRY'S INFRINGEMENT

74. BlackBerry has infringed and is continuing to infringe the '432 patent by making, using, selling and/or offering to sell in the United States, or importing into the United States, products or processes that practice the '432 patent in violation of 35 U.S.C. § 271(a), including without limitation BlackBerry Workspaces.

75. BlackBerry's infringement of the '432 patent has caused and will continue to cause damage for which Facebook is entitled to recovery under 35 U.S.C. § 284.

76. As set forth below, BlackBerry infringes the '432 patent. The following description is exemplary and illustrative of BlackBerry's infringement based on publicly available information. Facebook expects to further develop the evidence of BlackBerry's infringement after obtaining discovery from BlackBerry in the course of this action.

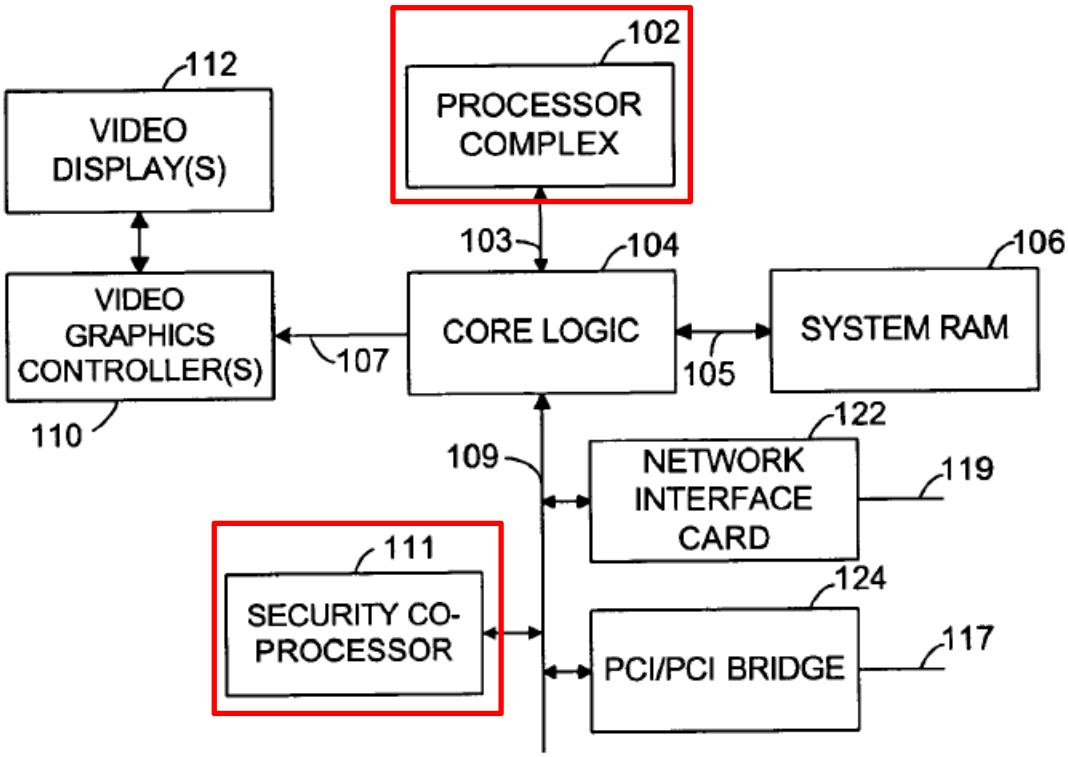
77. BlackBerry's WorkSpaces product, formerly called WatchDox, provides secure file sharing to users and organizations. The product can be hosted in a cloud implementation. An illustrative diagram of the WatchDox architecture is reproduced below, illustrating how files provided to the server are converted and validated by a security processing function and then placed into a secure repository, where the files may be further processed and accessed by remote devices.



(Source: WatchDox Security White Paper, at 5.)

78. An excerpt from an exemplary figure in the '432 patent is reproduced below, with red box annotations around exemplary processor complex **102** and exemplary security co-processor **111**.

('432, Fig. 2 (annotated excerpt).)



79. An illustrative description of BlackBerry's infringement on an element-by-element basis is provided below for exemplary claims of the patent.

- *1[p]. A method of providing security for a computer system, the method comprising the acts of:*

BlackBerry Workspaces involves a method of providing security for a computer system. BlackBerry provides a cloud hosting service. BlackBerry's product provides a secure file management platform. The platform separates security processing from other functionality such as the web application that serves users.

> The Workspaces virtual appliance is a multi-tier application with strict separation between the web application serving the users, the database that contains the system meta-data, and a secure file system that contains the encrypted documents.

(Source: http://help.blackberry.com/en/blackberry-workspaces-appliance-x/current/whitepaper/mbf1465305286684.html)

> The Workspaces next-generation virtual appliance is a composite system consisting of multiple virtual machines. These virtual machines are responsible for the system's front-end web and management interfaces, load balancing, document converters, and other internal components.
>
> The Workspaces virtual appliance virtual machines run hardened Redhat Enterprise Linux and one or more instances of Windows Server.
>
> File storage for the virtual appliance installation is a NAS, SAN, NFS, or an externally deployed Object-Storage. This component stores the encrypted customer files and the permissions database data.

(Source: http://help.blackberry.com/en/blackberry-workspaces-appliance-x/current/whitepaper/iip1465304150551.html)

> Introduction to BlackBerry Workspaces
>
> Welcome to BlackBerry Workspaces! If you're new to BlackBerry Workspaces, this guide provides useful tips to help you find your way around.
>
> **What is BlackBerry Workspaces?**
>
> BlackBerry Workspaces is a modern, highly secure, file management platform that enables effortless synchronization and secured sharing across multiple devices. BlackBerry Workspaces limits the risk for data loss or theft by embedding Digital Rights Management (DRM) security into every file, so your content remains secure and within your control, even after it is downloaded and shared with others.
>
> BlackBerry Workspaces can be accessed via your browser, or you can download our application to your PC or Mac, and your iOS, Android, or BlackBerry 10 device.
>
> Using the web or client applications, you can easily open, edit, annotate, and share. All your content is synchronized across all devices when they are online. Create workspaces and folders to organize your files, and manage access to them.

(Source: http://help.blackberry.com/en/blackberry-workspaces/current/quick-start-guide/vix1490520108806.html)

- *1[a]. generating a request for a file;*

BlackBerry Workspaces generates a request for a file, such as via a file access request (e.g., an open, edit, annotate or share request) based on a user request originated via a web browser or through the Workspaces client application. On the Workspaces server side, a request is generated that results in the requested document being converted

into a format for delivery to the user. For example, the system provides a secure Workspaces API call.

High Level System Workflow

Documents protected by BlackBerry Workspaces are secured at all times — at rest, in motion, and in-use. The Workspaces system works as follows:

1. Files are uploaded to the Workspaces servers over an encrypted SSL connection. These files may be uploaded via the Workspaces web interface, synchronized from a local folder, or potentially drawn from various enterprise systems, such as Outlook or SharePoint.

2. When a user requests to view a document, he or she is prompted to authenticate (if not already authenticated). Authentication may involve a username and password, email answer-back to verify the user's identity, or may be integrated with enterprise multi-factor or single-sign-on (SSO) systems. (See 'User Authentication' section for additional information). Once the Workspaces server has validated the authentication credentials, the user is authorized to view the document.

3. The requested document is then converted into one of several different formats, so it is optimized for high fidelity rendering on the device that is requesting it: an online web browser, PC, iPhone/iPad, BlackBerry, desktop system, etc. (See 'Device-optimized rendering' for more information.) These documents are then encrypted using industry standard 256-bit Advanced Encryption Standard (AES) encryption with Workspaces viewers and native apps and 128-bit AES as required by MS Office WDRM.

4. When an authorized user accesses a document via a web browser, the file is presented using Workspaces' secure online viewer.

(Source: https://idency.com/wp-content/uploads/2017/06/5bbc8123-541e-4e1b-995e-1e01eebb2ce5_wp-ensuring-document-security-across-any-device-with-workspaces.pdf (highlighting added))

All content, including meta-data, is encrypted and stored in a secure volume. This volume is accessible only via secure Workspaces API calls. Firewalls, monitoring, and other security tools are used to inspect the content residing on the server and to mask it from the outside.

(Source: https://idency.com/wp-content/uploads/2017/06/5bbc8123-541e-4e1b-995e-1e01eebb2ce5_wp-ensuring-document-security-across-any-device-with-workspaces.pdf)

Introduction to BlackBerry Workspaces

Welcome to BlackBerry Workspaces! If you're new to BlackBerry Workspaces, this guide provides useful tips to help you find your way around.

What is BlackBerry Workspaces?

BlackBerry Workspaces is a modern, highly secure, file management platform that enables effortless synchronization and secured sharing across multiple devices. BlackBerry Workspaces limits the risk for data loss or theft by embedding Digital Rights Management (DRM) security into every file, so your content remains secure and within your control, even after it is downloaded and shared with others.

BlackBerry Workspaces can be accessed via your browser, or you can download our application to your PC or Mac, and your iOS, Android, or BlackBerry 10 device.

Using the web or client applications, you can easily open, edit, annotate, and share. All your content is synchronized across all devices when they are online. Create workspaces and folders to organize your files, and manage access to them.

(Source: http://help.blackberry.com/en/blackberry-workspaces/current/quick-start-guide/vix1490520108806.html)

Download files

If you are the workspace owner or administrator, or the file owner, you can download the original file (without any access restrictions controlled by BlackBerry Workspaces) or the protected versio of it (with access protected by the BlackBerry Workspaces permissions).

> ***Note:*** *If you are not the owner or an administrator, and the file permissions do not permit unprotected downloading, you are able to download a protected version only.*

1. Locate the file that you want to download.
2. Do one of the following:
   - Hover over the file that you want to download, and then click **Download**. The file is downloaded with the highest level of permissions you have for your role in this folder.
   - Select the file in the content list, and in the action toolbar, click ⬇ and choose **Full Access** or **Protected**.
   - Locate the file and click ⋮ > and choose **Download - Full Access** or **Download - Protected**.

The file is downloaded to your computer. If you chose to download a "Full access" copy of the file, an unprotected copy is downloaded, and your actions on the file are not traced by BlackBerry Workspaces. If you chose to download a "protected" copy, your ability to view, edit, print or copy the content is determined by your user permissions for the file.

(Source: http://help.blackberry.com/en/blackberry-workspaces/current/user-guide/gry1443705389220.html)

- *1[b]. receiving the request at a dedicated security processor;*

BlackBerry Workspaces receives file access requests at a dedicated security processor. A Workspaces server application receives the request, which results in the dedicated security processor converting the file into a format for the user. The secure file system may receive the request as a secure API call.

> 3. The requested document is then converted into one of several different formats, so it is optimized for high fidelity rendering on the device that is requesting it: an online web browser, PC, iPhone/iPad, BlackBerry, desktop system, etc. (See 'Device-optimized rendering' for more information.) These documents are then encrypted using industry standard 256-bit Advanced Encryption Standard (AES) encryption with Workspaces viewers and native apps and 128-bit AES as required by MS Office WDRM.

(Source: https://idency.com/wp-content/uploads/2017/06/5bbc8123-541e-4e1b-995e-1e01eebb2ce5_wp-ensuring-document-security-across-any-device-with-workspaces.pdf (highlighting added))

> All content, including meta-data, is encrypted and stored in a secure volume. This volume is accessible only via secure Workspaces API calls. Firewalls, monitoring, and other security tools are used to inspect the content residing on the server and to mask it from the outside.

(Source: https://idency.com/wp-content/uploads/2017/06/5bbc8123-541e-4e1b-995e-1e01eebb2ce5_wp-ensuring-document-security-across-any-device-with-workspaces.pdf)

Service FQDN	The URL that you use to access the BlackBerry Workspaces application. This URL MUST correspond to SSL certificates and must consist of at least 3 parts. (e.g. *watchdox.nycompany.com*)
SSL Certificate / Chain / Private Key	SSL Certificates corresponding to the service FQDN.

(Source: http://help.blackberry.com/en/blackberry-workspaces-appliance-x/current/installation-and-upgrade/gem1464691870923.html, section "Install Appliance-X on Linux", step 8.)

Sizing requirements

Each deployment option has specific sizing recommendations that are based on server size, which are defined by server storage, memory, and the number of processors.

Table 1. Server sizes

Server size	Local operating system storage	Memory	Processors (CPU/vCPU)
Small	100GB	4 GB	2
Medium	100GB	8 GB	4
Large	100GB	12 GB	6
X-Large	100GB	16 GB	8

(Source: http://help.blackberry.com/en/blackberry-workspaces-appliance-x/current/

installation-and-upgrade/gem1464691870923.html)

- *1[c]. using the dedicated security processor to access the file;*

BlackBerry Workspaces uses the dedicated security processor to access the files in the Workspaces. For example, the system accesses the file in order to convert it into a particular format for the requesting user.

> 3. The requested document is then converted into one of several different formats, so it is optimized for high fidelity rendering on the device that is requesting it: an online web browser, PC, iPhone/iPad, BlackBerry, desktop system, etc. (See 'Device-optimized rendering' for more information.) These documents are then encrypted using industry standard 256-bit Advanced Encryption Standard (AES) encryption with Workspaces viewers and native apps and 128-bit AES as required by MS Office WDRM.

(Source: https://idency.com/wp-content/uploads/2017/06/5bbc8123-541e-4e1b-995e-1e01eebb2ce5_wp-ensuring-document-security-across-any-device-with-workspaces.pdf)

- *1[d]. using the dedicated security processor to validate the requested file;*

BlackBerry Workspaces uses the dedicated security processor to validate the requested file. As part of converting the file to a format for the requesting user, the system validates the requested file, for example to ensure that the file conversion has completed successfully. The system also will, for example, provide information on any file which failed to synchronize correctly, indicating that it has attempted to validate that file and found an error.

> 3. The requested document is then converted into one of several different formats, so it is optimized for high fidelity rendering on the device that is requesting it: an online web browser, PC, iPhone/ iPad, BlackBerry, desktop system, etc. (See 'Device-optimized rendering' for more information.) These documents are then encrypted using industry standard 256-bit Advanced Encryption Standard (AES) encryption with Workspaces viewers and native apps and 128-bit AES as required by MS Office WDRM.

(Source: https://idency.com/wp-content/uploads/2017/06/5bbc8123-541e-4e1b-995e-1e01eebb2ce5_wp-ensuring-document-security-across-any-device-with-workspaces.pdf)

> View a list of sync errors
>
> **Before you begin:** If there was a problem syncing your files, an item appears in the taskbar menu.
>
> 1. Right-click the Workspaces icon in the taskbar, and select ***x* Sync error(s)**. The BlackBerry Workspaces Sync Errors window appears.
> 2. Click the file name to locate the file.
> 3. If available, click the suggested solution to solve the issue.
> 4. Click ⓘ to view more information about the error and the suggested solution.
> 5. Follow the instructions in the solution to remove the error.

(Source: http://help.blackberry.com/en/blackberry-workspaces-for-windows/current/user-guide/gry1443705752000.html)

- *1[e]. providing the file to an other processor, if the requested file is validated;*

BlackBerry Workspaces provides the file to another processor if the requested file is validated. For example, the Workspaces system will provide the converted and

validated file to a web application (e.g., a web server with processor) to be provided to the user. The system may also provide a file to a user's device, such as a BlackBerry smartphone containing a processor.

> 3. The requested document is then converted into one of several different formats, so it is optimized for high fidelity rendering on the device that is requesting it: an online web browser, PC, iPhone/iPad, BlackBerry, desktop system, etc. (See 'Device-optimized rendering' for more information.) These documents are then encrypted using industry standard 256-bit Advanced Encryption Standard (AES) encryption with Workspaces viewers and native apps and 128-bit AES as required by MS Office WDRM.
>
> 4. When an authorized user accesses a document via a web browser, the file is presented using Workspaces' secure online viewer.

(Source: https://idency.com/wp-content/uploads/2017/06/5bbc8123-541e-4e1b-995e-1e01eebb2ce5_wp-ensuring-document-security-across-any-device-with-workspaces.pdf (highlighting added))

> The Workspaces virtual appliance is a multi-tier application with strict separation between the web application serving the users, the database that contains the system meta-data, and a secure file system that contains the encrypted documents.

(http://help.blackberry.com/en/blackberry-workspaces-appliance-x/current/whitepaper/mbf1465305286684.html)

File storage

When files are downloaded from the BlackBerry Workspaces server for viewing, they are cached in a secure cache on your device that is accessible only by BlackBerry Workspaces app for iOS. This cache is not synced or backed up by iTunes or iCloud. Furthermore, the file is stored in this cache in encrypted form. The keys to decrypt the file are stored separately and are themselves stored in encrypted format.

(Source: https://help.blackberry.com/en/blackberry-workspaces-app-for-android/current/user-guide/gry1443705134196.html)

- *1[f].validating a user access to execute the request; and*

BlackBerry Workspaces validates a user's access to a file, executing the access request only if the user is authorized. The system checks to confirm that the user requesting the file has been authorized to execute the request.

4. When an authorized user accesses a document via a web browser, the file is presented using Workspaces' secure online viewer.

(Source: https://idency.com/wp-content/uploads/2017/06/5bbc8123-541e-4e1b-995e-1e01eebb2ce5_wp-ensuring-document-security-across-any-device-with-workspaces.pdf (highlighting added))

Managing access

The **Permissions** tab is displayed for a selected workspace, folder, or file, when you are an administrator in the workspace. As workspace administrator, you can manage who can access workspace items. New members can be added as individuals, by defining an email domain, or as a Microsoft Active Directory or regular group. For each member or group of members, you can set their role and access permissions for a selected workspace, folder, or files. If necessary, you can edit the roles and permissions.

For more information on the meaning of user roles and permissions, including customized access to folders and files, see About user roles and permissions.

(Source: http://help.blackberry.com/en/blackberry-workspaces/current/user-guide/gry1443705314525.html)

About permissions

Use permissions to define user access rights for workspace files. A number of permission sets are available, depending on what has been set by your organization BlackBerry Workspaces administrator, and according to your organization's defined enterprise mode.

(Source: http://help.blackberry.com/en/blackberry-workspaces/current/user-guide/gry1443705301815.html)

- *1[g]. enabling the other processor to continue processing the file, if the user access is validated.*

BlackBerry Workspaces enables the other processor to continue processing the file if the user's access is validated. For example, the web application processor is enabled to continue processing the file if the user access request is validated, by permitting the file to be served to the user.

4. When an authorized user accesses a document via a web browser, the file is presented using Workspaces' secure online viewer.

(Source: https://idency.com/wp-content/uploads/2017/06/5bbc8123-541e-4e1b-995e-1e01eebb2ce5_wp-ensuring-document-security-across-any-device-with-workspaces.pdf (highlighting added))

Managing access

The **Permissions** tab is displayed for a selected workspace, folder, or file, when you are an administrator in the workspace. As workspace administrator, you can manage who can access workspace items. New members can be added as individuals, by defining an email domain, or as a Microsoft Active Directory or regular group. For each member or group of members, you can set their role and access permissions for a selected workspace, folder, or files. If necessary, you can edit the roles and permissions.

For more information on the meaning of user roles and permissions, including customized access to folders and files, see About user roles and permissions.

(Source: http://help.blackberry.com/en/blackberry-workspaces/current/user-guide/gry1443705314525.html)

Available permission sets

Full access

Users with full access permissions can perform all actions in BlackBerry Workspaces.

(Source: https://help.blackberry.com/en/blackberry-workspaces-for-windows/current/user-guide/gry1443705302406.html)

- *3. The method, as set forth in claim 1, wherein accessing the file comprises loading the file from a system memory.*

On information and belief, the step of accessing the file comprises loading the file from a system memory, such as RAM memory at a server.

- *5. The method, as set forth in claim 1, wherein the dedicated security processor is in a remote computer system.*

As shown above for Claim 1, the dedicated security processor in a WorkSpaces implementation may be in a remote computer system, such as a cloud-based implementation where the security processing is performed in a computer system remote from the other processor.

- *6. The method, as set forth in claim 1, wherein the other processor and the dedicated security processor are disposed in a computer system.*

As shown above for Claim 1, the dedicated security processor and other processor in a WorkSpaces implementation may be disposed in a computer system, such as a WorkSpaces cloud or server computer system.

80. Facebook is entitled to relief as a result of BlackBerry's infringement, including without limitation monetary damages no less than a reasonable royalty.

COUNT V: INFRINGEMENT OF U.S. PATENT NO. 6,744,759

81. Facebook incorporates by reference and re-alleges all foregoing paragraphs of this Complaint as if fully set forth herein.

82. Facebook is the owner by assignment of U.S. Patent No. 6,744,759 ("'759 patent"), entitled "System and method for providing user-configured telephone

service in a data network telephony system," including the exclusive right to bring suit to enforce the patent and the exclusive right to obtain relief for infringement. The '759 patent was duly and legally issued by the U.S. Patent and Trademark Office on June 1, 2004. The patent is based on U.S. Patent Application Ser. No. 09/405,283 filed on September 27, 1999.

83. A true and correct copy of the '759 patent is attached as Exhibit E.

84. The '759 patent is valid and enforceable under the United States Patent Laws.

SUMMARY OF INVENTION

85. The '759 patent originated with network technology company 3Com Corporation ("3Com"), based in Santa Clara, California. 3Com was recognized as one of the market leaders in networking hardware and software products including Voice over IP (VoIP) telephony products. As of the patent filing date in 1999, 3Com reported that it had more than 200 million customers worldwide. 3Com was acquired by HP in 2010 for a reported value of approximately $2.7 billion.

86. The '759 patent addresses needs that arose in the field of telephone service configuration. The patent explains that telephone service providers could "permit customer subscribers of the features to tailor their telephone service according to individual needs" with services such as call blocking, caller ID, and call forwarding. ('759, col. 1:25-27.) However, while telephone service features were available, "the features are nevertheless limited in their flexibility and scope. The effect to the user is that the features become clumsy and difficult to use." (*Id.*, col. 2:38-39.) "For example, in order to use the Call Forwarding function, the user must perform the steps at the user's own phone prior to moving to the location of the telephone to which calls will be forwarded." (*Id.*, col. 2:41-44.)

87. In addition, telephone devices themselves suffered from deficiencies. For example, although the Public Switched Telephone Network (PSTN) had been developed, "[o]ne problem with the PSTN is that the terminal devices (e.g. telephones)

lack intelligence and operate as 'dumb' terminals on a network having the intelligence in central offices." (*Id*., col. 2:49-52.) While some PSTN telephones included display features, they were "limited however by the closed PSTN signaling architecture, which prohibits access by the PSTN telephones to the network signaling protocols." (*Id*., col. 2:61-64.) Furthermore, "[t]he display functions are effectively limited to displaying text, again, as a 'dumb' terminal." (*Id*., col. 2:64-65.)

88. Beyond traditional PSTN telephony, Internet telephony was also known, which could involve telephones that "may be substantially more intelligent than typical PSTN telephones" and "may include substantially the computer resources of a typical personal computer." (*Id*., col. 3:19-22.)

89. The '759 patent explains that needs existed in the field, including needs for incorporating feature sets "into a data network telephony system that uses a data network such as the Internet," providing "new features and enhancements to telephony service that accommodates and conforms to users' needs," and providing "features and capabilities to telephone service that create new opportunities for users and for service providers." (*Id*., col. 3:24-31.)

90. The inventions taught by the '759 patent addressed these needs, as described by the patent. The patent states:

> The present invention addresses the above needs by providing a system in a data network telephony system, such as for example, the Internet, that provides a way for users to make brand new telephones usable without having to wait while the telephone company programs an account. The embodiments of the present invention may also be used to modify existing telephone accounts to incorporate new features, or features that may be desired for a limited amount of time.

(*Id*., col. 3:32-40.)

91. According to the patent, "[o]ne advantage of the present invention is that telephone features become user-configurable." (*Id*., col. 3:41-42.) "Another advantage is that the extent to which features are user-configurable may be determined by the

service provider. The service provider may wish to make a few basic features standard and impose their use in a registration function. Other features may then be made selectable by the user." (*Id*., col. 3:43-48.)

92. The specification describes illustrative examples of how the invention may be implemented using data network telephones and telephony features that the user may select by accessing a service provider's web page. (*Id*., col. 16:6-8, 16:16-39.) In addition to features selected when "setting up a new account," features may also be modified based on the user's selections, so that "[u]sers need not be locked into any service plan or feature set." (*Id*., col. 11:20-25.) "One advantage of such provisioning functions is that services may be ordered for temporary use in a manner that is convenient to the user." (*Id*., col. 11:25-28.)

93. The specification also describes another "advantage" of the disclosed inventive system that the user can "obtain access to fully personalized, user-configured service account as well as to user-selected telephony enhancements and features." (*Id*., col. 6:55-58.)

94. The claims of the '759 patent reflect the improvements and benefits taught by the specification. For example, each claim of the patent recites functionality through which a service provider can enable a user, using a form presented in the web browser, to request certain features to be provisioned for a data network telephone. As taught by the specification, the inventions recited in the claims thus enable a service provider to allow users to select and modify certain user-configurable features for a data network telephone in a convenient manner using a web-based interface, where the service provider can determine which available features are user-configurable. As the specification explains, these inventions for user-configurable data network telephone features enable a user to conveniently select and configure features for the data network telephone without the user having to wait for the telephone company or service provider to program the user's account. Further incorporating these benefits taught by the patent, claims 4 and 8 and the claims that depend therefrom further specify that the service

provider sends a message to the data network telephone effectuating the features chosen by the user.

BLACKBERRY'S INFRINGEMENT

95. BlackBerry has infringed and is continuing to infringe the '759 patent by making, using, selling and/or offering to sell in the United States, or importing into the United States, products or processes that practice the '759 patent in violation of 35 U.S.C. § 271(a), including without limitation the BlackBerry Enterprise Server (BES, including versions BES10 – BES12) and the BlackBerry Unified Endpoint Manager (UEM).

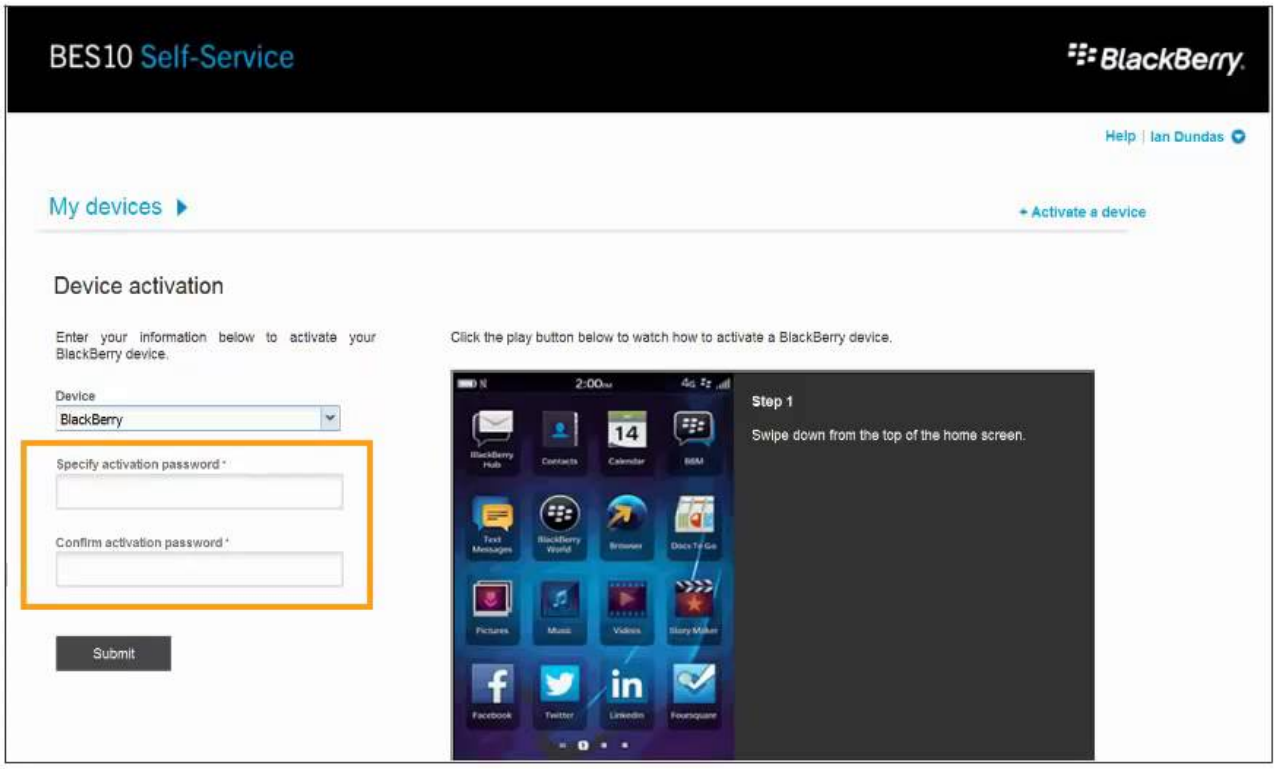
96. BlackBerry's infringement of the '759 patent has caused and will continue to cause damage for which Facebook is entitled to recovery under 35 U.S.C. § 284.

97. As set forth below, BlackBerry infringes the '759 patent. The following description is exemplary and illustrative of BlackBerry's infringement based on publicly available information. Facebook expects to further develop the evidence of BlackBerry's infringement after obtaining discovery from BlackBerry in the course of this action.

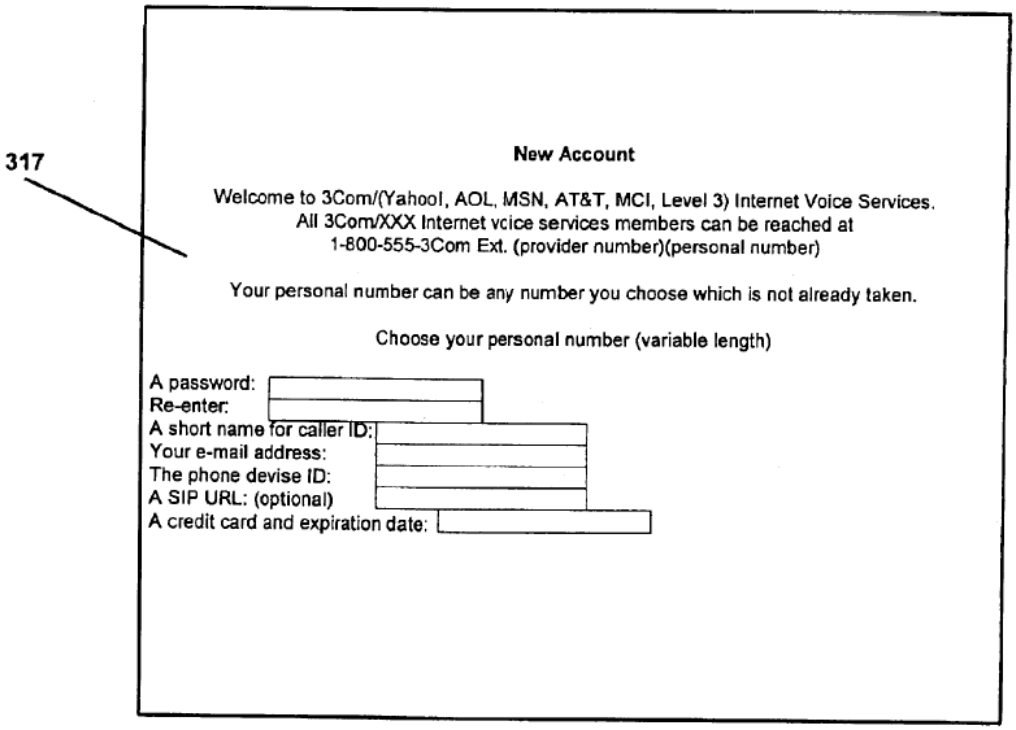
98. BlackBerry's UEM product and predecessor BES product include a Self-Service feature, which is a web-based application enabling users to perform certain tasks, such as creating a password to activate a device or sending commands to the device. If a user's device is lost or stolen, the user can perform actions through the Self-Service interface such as remotely changing the password on the device or deleting data from the device.

99. The following is an exemplary video screenshot provided by BlackBerry, showing how a user can specify an activation password for a device using the Self-Service web interface.

(Source: https://www.youtube.com/watch?v=F7e-LmFyWXw)



100. The following figure from the '759 patent shows an exemplary web interface where a user can specify information as part of the process to provision features for a data network telephone.



('759, Fig. 4B.)

101. An illustrative description of BlackBerry's infringement on an element-by-element basis is provided below for exemplary claims of the patent.

- *8[p]. A method for providing a user selected configuration for a data network telephone comprising the steps of:*

The BES and BlackBerry UEM Self-Service websites allow the user to select a configuration for a data network telephone. The Self-Service feature works for smartphones that are data network phones that enable telephony over data networks, such as Voice Over Wi-Fi and Voice Over LTE.

> BES12 Self-Service is a web-based application that you can use to perform certain tasks, such as creating a password to activate your device or sending commands to your device. If your device is lost or stolen, you can remotely change the password on your device or delete data from your device. You don't need to install any software on your computer to use

> BES12 Self-Service. Your administrator will provide you with the web address and login information that you need to log in to BES12 Self-Service.

(Source: http://help.blackberry.com/en/bes12-self- service/latest/bes 12-self-service/amo1375906210935.html)

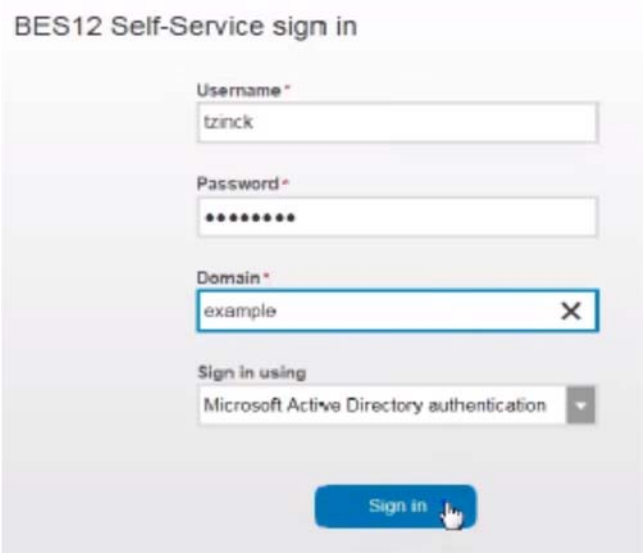
> What is BlackBerry UEM Self-Service?
>
> BlackBerry UEM Self-Service is a web-based application that you can use to perform certain tasks, such as creating a password to activate your device or sending commands to your device. If your device is lost or stolen, you can remotely change the password on your device or delete data from your device. You don't need to install any software on your computer to use BlackBerry UEM Self-Service. .
>
> Your administrator will provide you with the web address and login information that you need to log in to BlackBerry UEM Self-Service

(Source: http://help.blackberry.com/en/blackberry-uem-self-service/latest/blackberry-uem-self-service/amo1375906210935.html)

(Source: https://us.blackberry.com/support/business/blackberry-uem)

- *8[a]. receiving a request to configure the data network telephone from the user;*

After the user logs into the BES12 or UEM Self-Service website and provides a configuration request, a request is received to configure the user's data network telephone.



(Source: https://www.youtube.com/watch?v=Hydk1TFK54I)

Create an activation password or QR Code

Note: If your organization uses BlackBerry UEM Cloud, QR codes are not available.

To activate devices, you need an activation password or a QR Code. Depending on the permissions that your administrator has configured in BlackBerry UEM, you might be able to create an activation password or a QR Code using BlackBerry UEM Self-Service.

1. Log in to BlackBerry UEM Self-Service.
2. Depending on whether you are activating your first device, or you already have an activated device, click + or click + > **Activate a device**.
3. In the **Device** drop-down menu, select the type of device that you want to activate.
4. In the **Specify activation password** and **Confirm activation password** fields, type a password that complies with the specified requirements.
5. Click **Submit**.
6. Review the information that is displayed in the confirmation message.
   - If an Activation URL is displayed, copy it for later. You need to type the URL when you activate your device.
   - If a QR Code is displayed, you can use it to activate your device. For instructions, see Activate a device using a QR code. If necessary you can screen capture the image to use later.
7. Click **Close**.

(Source: http://help.blackberry.com/en/blackberry-uem-self-service/latest/blackberry-uem-self-service-pdf/BlackBerry-UEM-Self-Service-latest-User-Guide-en.pdf)

Activate a BlackBerry 10 device

You can activate your BlackBerry 10 device to associate it with your organization's environment so that you can access work data on your device.

Before you begin:

- In BlackBerry UEM Self-Service, Create an activation password or QR Code.
- Watch a video tutorial available at help.blackberry.com/detectLang/activation-videos.

1. On the device, navigate to **Settings**.
2. Tap **Accounts**.
3. If you have existing accounts on this device, tap **Add Account**. Otherwise, continue to Step 4.
4. Tap **Email, Calendar and Contacts**.
5. Type your work email address and tap **Next**.
6. In the **Password** field, type the activation password you received. Tap **Next**.
7. If you receive a warning that your device could not look up connection information, complete the following steps:
   a. Tap **OK**.
   b. Tap **Advanced**.
   c. Tap **Work Account**.
   d. In the **Server Address** field, type the server address. Tap **Done**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
8. Follow the instructions on the screen to complete activation.

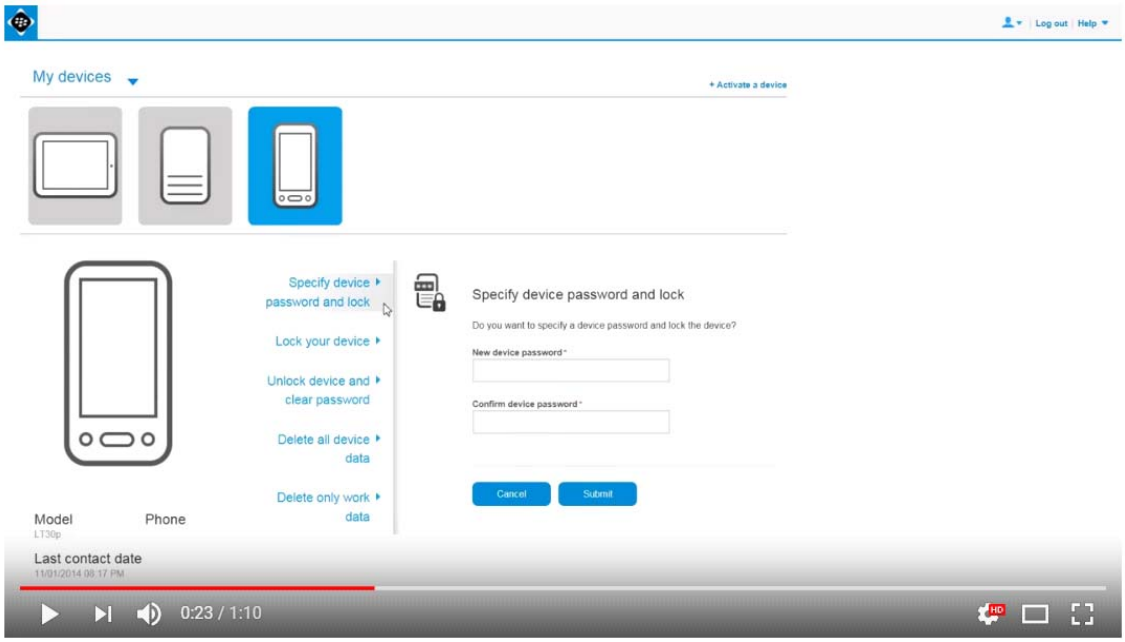
After you finish: To verify that the activation process completed successfully, perform one of the following actions:

- On the device, navigate to the BlackBerry Hub and confirm that the email address is present. Navigate to the Calendar and confirm that the appointments are present.
- In BlackBerry UEM Self-Service, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.

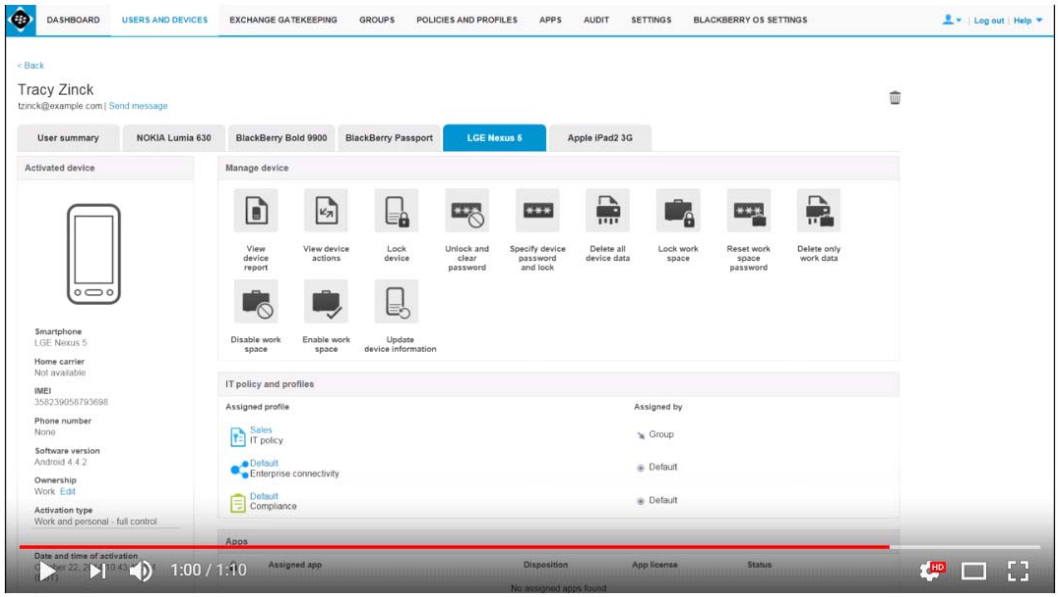
(Source: http://help.blackberry.com/en/blackberry-uem-self-service/latest/blackberry-uem-self-service-pdf/BlackBerry-UEM-Self-Service-latest-User-Guide-en.pdf)

- *8[b]. presenting a user feature request form in a web browser of a workstation, the user feature request form prompting the user to select features with which the data network telephone is to be provisioned;*

The user is presented with features in a request form prompting selection of commands with which their data network telephone is to be provisioned. For example, the web browser form prompts the user to select features such as (1) specifying a device password and locking the device, (2) unlocking the device and clearing password, and other features. The user can select the features of specifying a password and locking the device, for example, to provision the device with the features of a password and being locked.



(Source: https://www.youtube.com/watch?v=Hydk1TFK54I)



(Source: https://www.youtube.com/watch?v=Hydk1TFK54I)

Using BES12 Self-Service, you can send various remote commands to your device. For example:

- If your device is lost or stolen, you can remotely lock the device or delete data from the device.

- If you forget the device password on your iOS or Android device, you can clear it.
- If you misplace your iOS, Android, or Windows 10 Mobile device, you might be able to use BES12 Self-Service to locate your device on a map"

(Source: http://help.blackberry.com/en/bes12-self-service/latest/bes_12-self-service-pdf/BES12-Self-Service-latest-User-Guide-en.pdf)

Set a device password and lock the device

If you have a BlackBerry 10, Android, or Windows device, you can lock your device remotely and set or reset a device password. The device is locked and can be unlocked with the new password.

If you have an OS X device, you must set a 6-digit PIN. The device restarts and cannot be accessed without entering the PIN.

1. In BlackBerry UEM Self-Service, select the device that you want to lock.
2. For BlackBerry 10 devices, complete the following steps:
   a. Click **Specify device password and lock**.
   b. Type and confirm a new device password, and click **Submit**.
3. For Android or Windows devices, complete the following steps:
   a. Click **Generate device password and lock**.
   b. Type your email address and click **Generate**.
4. For OS X devices, complete the following steps:
   a. Click **Lock device using PIN**.
   b. Type a PIN and click **Submit**.

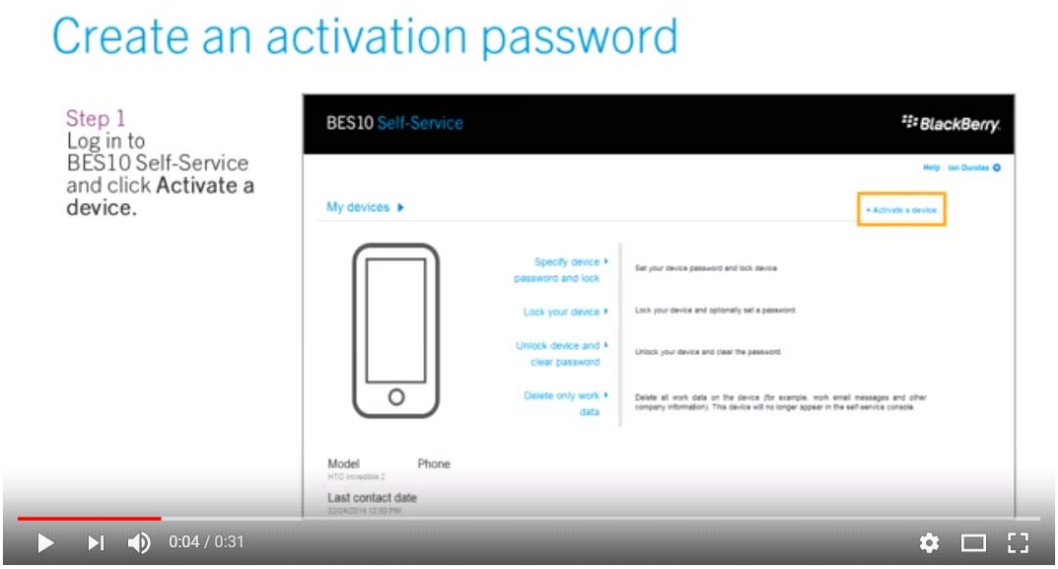
(Source: http://help.blackberry.com/en/blackberry-uem-self-service/latest/blackberry-uem-self-service-pdf/BlackBerry-UEM-Self-Service-latest-User-Guide-en.pdf)

Delete all device data

If your device is lost or stolen, you might want to remotely delete all the data on your device. This command wipes all data from the device, return the device to its factory settings, and deactivates it from BlackBerry UEM. The device will no longer appear in the BlackBerry UEM Self-Service console. For OS X devices you also set a PIN when you delete all device data.

1. In BlackBerry UEM Self-Service, select the device.
2. Click **Delete all device data**.
3. To confirm your request, click **Delete all device data**.

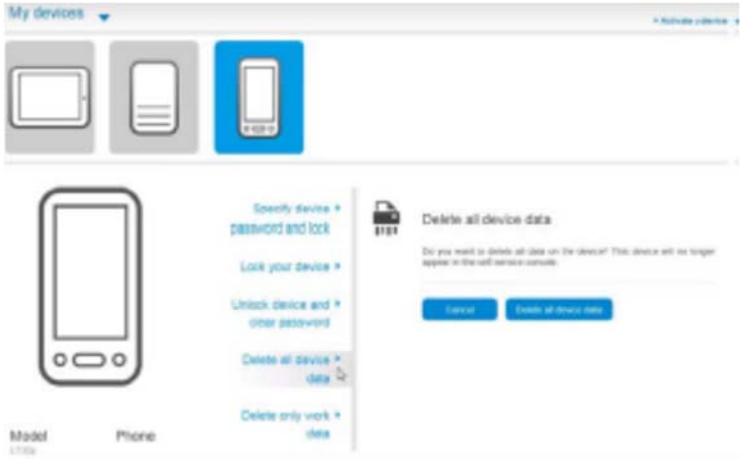
(Source: http://help.blackberry.com/en/blackberry-uem-self-service/latest/blackberry-uem-self-service-pdf/BlackBerry-UEM-Self-Service-latest-User-Guide-en.pdf)



(Source: https://www.youtube.com/watch?v=F7e-LmFyWXw)

- *8[c]. setting a user account in accordance with the selected features;*

Once the presented feature is selected by the user, the user account is set in accordance with the feature.



(Source: https://www.youtube.com/watch?v=Hydk1TFK54I)

> BES12 Self-Service is a web-based application that you can use to perform certain tasks, such as creating a password to activate your device or sending commands to your device. If your device is lost or stolen, you can remotely change the password on your device or delete data from your device. You don't need to install any software on your computer to use BES12 Self-Service. Your administrator will provide you with the web address and login information that you need to

log in to BES12 Self-Service.

(Source: https://help.blackberry.com/en/bes12-self-service/latest/bes12-self-service/amo1375906210935.html)

Set a device password and lock the device

If you have a BlackBerry 10, Android, or Windows device, you can lock your device remotely and set or reset a device password. The device is locked and can be unlocked with the new password.

If you have an OS X device, you must set a 6-digit PIN. The device restarts and cannot be accessed without entering the PIN.

1. In BlackBerry UEM Self-Service, select the device that you want to lock.
2. For BlackBerry 10 devices, complete the following steps:
   a. Click **Specify device password and lock**.
   b. Type and confirm a new device password, and click **Submit**.
3. For Android or Windows devices, complete the following steps:
   a. Click **Generate device password and lock**.
   b. Type your email address and click **Generate**.
4. For OS X devices, complete the following steps:
   a. Click **Lock device using PIN**.
   b. Type a PIN and click **Submit**.

(Source: http://help.blackberry.com/en/blackberry-uem-self-service/latest/blackberry-uem-self-service-pdf/BlackBerry-UEM-Self-Service-latest-User-Guide-en.pdf)

- *8[d]. sending a configuration message to provision the data network telephone with the features selected; and*

After the user account is set, a configuration message is sent to the data network telephone in order for the features to take effect on the device.

> BES12 Self-Service is a web-based application that you can use to perform certain tasks, such as creating a password to activate your device or sending commands to your device. If your device is lost or stolen, you can remotely change the password on your device or delete data from your device. You don't need to install any software on your computer to use BES12 Self-Service. Your administrator will provide you with the web address and login information that you need to log in to BES12 Self-Service.

(Source: https://help.blackberry.com/en/bes12-self-service/latest/bes 12-self-service/amo1375906210935.html)

Sending commands to your device

3

Using BlackBerry UEM Self-Service, you can send various remote commands to your device. For example:

- If your device is lost or stolen, you can remotely lock the device or delete data from the device.
- If you forget the device password on your iOS or Android device, you can clear it.
- If you misplace your iOS, Android, or Windows 10 Mobile device, you might be able to use BlackBerry UEM Self-Service to locate your device on a map.

Your device must be turned on and connected to a wireless network to receive commands that you send from BlackBerry UEM Self-Service. The commands that you can send depend on the type of device that you have. The following table summarizes the remote commands that you can send to devices:

(Source: http://help.blackberry.com/en/blackberry-uem-self-service/latest/blackberry-uem-self-service-pdf/BlackBerry-UEM-Self-Service-latest-User-Guide-en.pdf)

Set a device password and lock the device

If you have a BlackBerry 10, Android, or Windows device, you can lock your device remotely and set or reset a device password. The device is locked and can be unlocked with the new password.

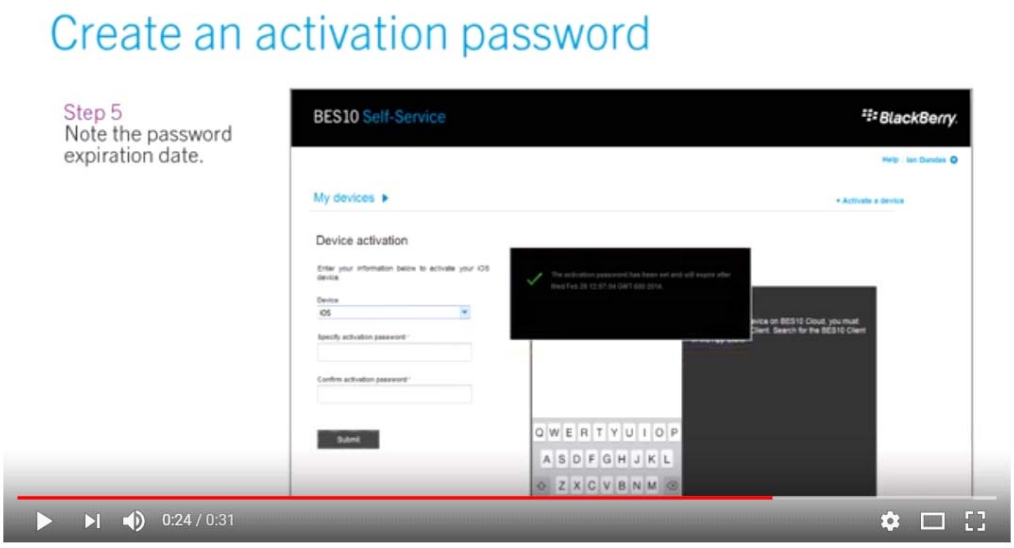
If you have an OS X device, you must set a 6-digit PIN. The device restarts and cannot be accessed without entering the PIN.

1. In BlackBerry UEM Self-Service, select the device that you want to lock.
2. For BlackBerry 10 devices, complete the following steps:
   a. Click **Specify device password and lock**.
   b. Type and confirm a new device password, and click **Submit**.
3. For Android or Windows devices, complete the following steps:
   a. Click **Generate device password and lock**.
   b. Type your email address and click **Generate**.
4. For OS X devices, complete the following steps:
   a. Click **Lock device using PIN**.
   b. Type a PIN and click **Submit**.

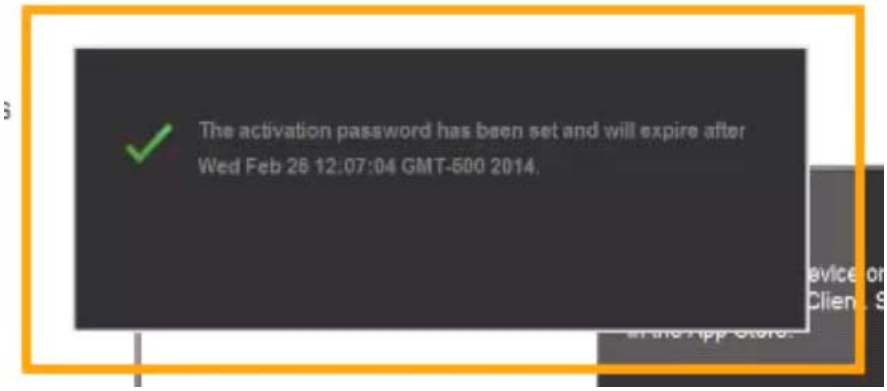
(Source: http://help.blackberry.com/en/blackberry-uem-self-service/latest/blackberry-uem-self-service/amo1377803743419.html)

- *8[e]. causing a confirming message to be presented to the user, the confirming message indicating to the user that the data network telephone is provisioned with the features selected by the user.*

The system causes a confirming message to be presented to the user indicating that the data network telephone is provisioned with the selected features. The message may be presented to the user at the Self-Service web interface and/or at the user's device, as per dependent claims 9 and 10, for example indicating that the device is locked, has its password set, or has other provisioned features.



(Source: https://www.youtube.com/watch?v=F7e-LmFyWXw)



(Source: https://www.youtube.com/watch?v=F7e-LmFyWXw)

Delete all device data

If your device is lost or stolen, you might want to remotely delete all the data on your device. This command wipes all data from the device, return the device to its factory settings, and deactivates it from BlackBerry UEM. The device will no longer appear in the BlackBerry UEM Self-Service console. For OS X devices you also set a PIN when you delete all device data.

1. In BlackBerry UEM Self-Service, select the device.
2. Click **Delete all device data**.
3. To confirm your request, click **Delete all device data**.

(Source: http://help.blackberry.com/en/blackberry-uem-self-service/latest/blackberry-uem-self-service-pdf/BlackBerry-UEM-Self-Service-latest-User-Guide-en.pdf)

Set a device password and lock the device

If you have a BlackBerry 10, Android, or Windows device, you can lock your device remotely and set or reset a device password. The device is locked and can be unlocked with the new password.

If you have an OS X device, you must set a 6-digit PIN. The device restarts and cannot be accessed without entering the PIN.

1. In BlackBerry UEM Self-Service, select the device that you want to lock.
2. For BlackBerry 10 devices, complete the following steps:
   a. Click **Specify device password and lock**.
   b. Type and confirm a new device password, and click **Submit**.
3. For Android or Windows devices, complete the following steps:
   a. Click **Generate device password and lock**.
   b. Type your email address and click **Generate**.
4. For OS X devices, complete the following steps:
   a. Click **Lock device using PIN**.
   b. Type a PIN and click **Submit**.

(Source: http://help.blackberry.com/en/blackberry-uem-self-service/latest/blackberry-uem-self-service/amo1377803743419.html)

- *9. The method of claim 8, wherein causing a confirming message to be presented to the user comprises sending a confirming message to the workstation that causes the workstation to present to the user the confirming message.*

The Self-Service feature causes a confirming message to be presented to the user, at the Self-Service web interface and/or at the user's device.

- *10. The method of claim 8 wherein causing a confirming message to be presented to the user comprises sending a confirming message to the data network telephone that causes the data network telephone to present to the user the confirming message.*

The Self-Service feature causes a confirming message to be presented to the user, at the Self-Service web interface and/or at the user's device.

102. Facebook is entitled to relief as a result of BlackBerry's infringement, including without limitation monetary damages no less than a reasonable royalty.

COUNT VI: INFRINGEMENT OF U.S. PATENT NO. 7,302,698

103. Facebook incorporates by reference and re-alleges all foregoing paragraphs of this Complaint as if fully set forth herein.

104. Facebook is the owner by assignment of U.S. Patent No. 7,302,698 ("'698 patent"), entitled "Operation of trusted state in computing platform," including the exclusive right to bring suit to enforce the patent and the exclusive right to obtain relief for infringement. The '698 patent was duly and legally issued by the U.S. Patent and Trademark Office on November 27, 2007. The patent is based on U.S. Patent Application Ser. No. 09/728,827 filed on November 28, 2000.

105. A true and correct copy of the '698 patent is attached as Exhibit F.

106. The '698 patent is valid and enforceable under the United States Patent Laws.

SUMMARY OF INVENTION

107. The '698 patent originated with the HP corporate family. Facebook refers to and incorporates by reference paragraph 68 above.

108. The '698 patent addresses computer security. As described in the patent, prior art operating systems before the '698 patent suffered from problems with security, such as vulnerability to viruses and unauthorized third-party modifications. ('698, col. 2:38-55.) One identified problem with prior art computing platforms was that "[t]he operating status of a computer system or platform and the status of the data within

the platform or system is dynamic and difficult to predict." (*Id*., col. 2:40-43.) As a result, "[i]t is difficult to determine whether a computer platform is operating correctly because the state of the computer platform and data on the platform is constantly changing and the computer platform itself may be dynamically changing." (*Id*., col. 2:42-46.)

109. To address the perceived problems, the invention of the '698 patent provides increased security to a computing system by using a monitoring component that operates to determine the current operational state of the system. The patent describes: "Specific embodiments of the present invention comprise a computer platform having a processing means and a memory means, and which is physically associated with a component, known herein after as a 'trusted component' which monitors operation of the computer platform by collecting metrics data from the computer platform, and which is capable of verifying to third party computer entities interacting with the computer platform to the correct functioning of the computer platform." (*Id*., col. 7:18-26.) The patent describes that security is enhanced by the use of a monitoring component in a number of ways:

> A user of a computing entity has higher confidence in the integrity and security of his/her own computer entity and in the integrity and security of the computer entity belonging to the other computing entity.
>
> Each entity is confident that the other entity is in fact the entity which it purports to be.
>
> Where one or both of the entities represent a party to a transaction, e.g. a data transfer transaction, because of the in-built trusted component, third party entities interacting with the entity have a high degree of confidence that the entity does in fact represent such a party.
>
> The trusted component increases the inherent security of the entity itself, through verification and monitoring processes implemented by the trusted component.

> The computer entity is more likely to behave in the way it is expected to behave.

(*Id*., col. 7:33-49.)

110. The claims of the '698 patent reflect these technological benefits that increase the security of the computer platform as described by the patent. For example, each claim recites the use of a "monitoring component" having a data processor and a memory, distinct from a first data processor and memory in a computer system, that performs functions including determining which operating state is the current operating state. As described in the specification, for example, the presence of a monitoring component increases the inherent security of the computing entity itself through the verification and monitoring processes that it implements.

BLACKBERRY'S INFRINGEMENT

111. BlackBerry has infringed and is continuing to infringe the '698 patent by making, using, selling and/or offering to sell in the United States, or importing into the United States, products or processes that practice the '698 patent in violation of 35 U.S.C. § 271(a), including without limitation its QNX software products, including the QNX Neutrino Realtime Operating System (RTOS), and related applications and implementations. QNX Neutrino is provided by BlackBerry for a variety of applications such as BlackBerry's CAR Infotainment products, the BlackBerry 10 OS operating system, and other applications.

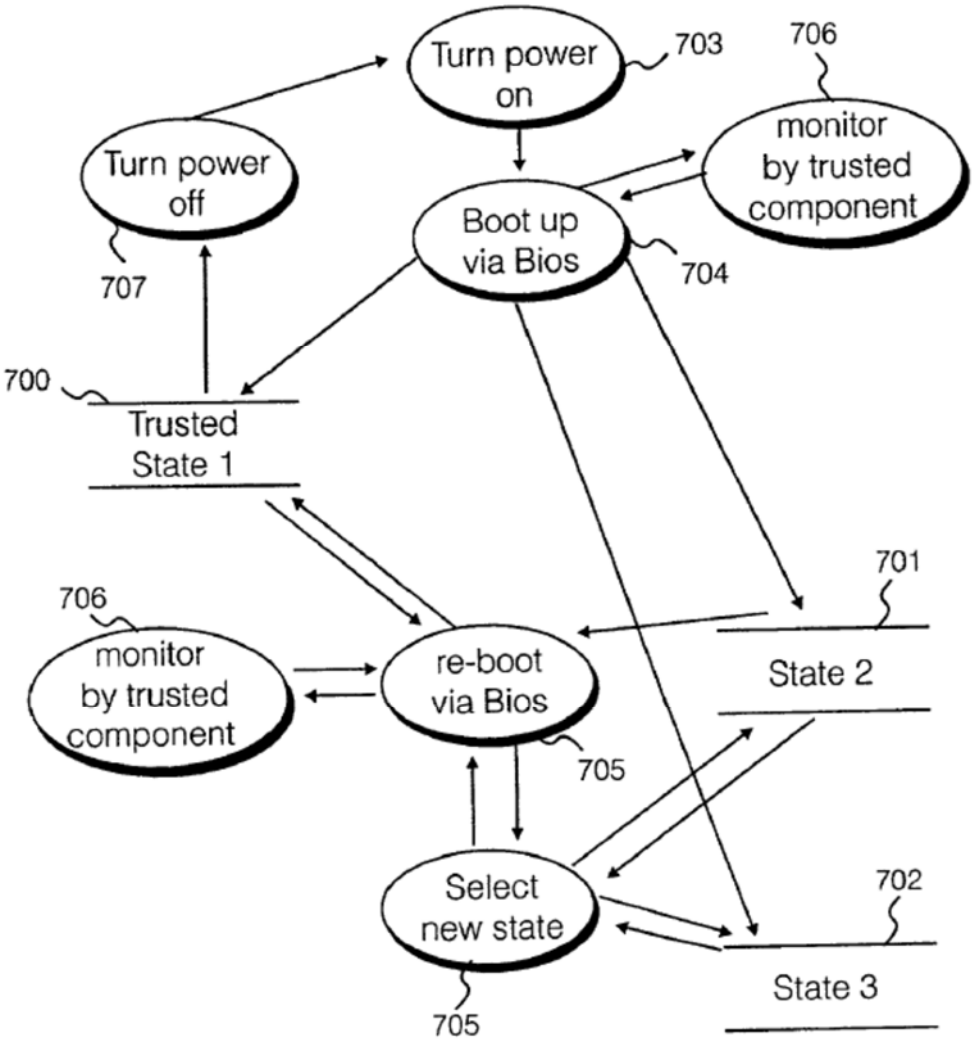
112. BlackBerry's infringement of the '698 patent has caused and will continue to cause damage for which Facebook is entitled to recovery under 35 U.S.C. § 284.

113. As set forth below, BlackBerry infringes the '698 patent. The following description is exemplary and illustrative of BlackBerry's infringement based on publicly available information. Facebook expects to further develop the evidence of BlackBerry's infringement after obtaining discovery from BlackBerry in the course of this action.

114. BlackBerry's QNX Neutrino uses monitoring components to monitor

operating states of a computing platform. For example, High Availability Manager ("HAM") components monitor operating states so that appropriate action can be taken if needed. The HAM contains subcomponents such as entities, conditions, and actions and may also be associated with a Guardian. According to BlackBerry, the HAM provides "a resilient manager (or 'smart watchdog') that can perform multistage recovery whenever system services or processes fail, no longer respond, or are detected to be in a state where they cease to provide acceptable levels of service." (Source: http://support7.qnx.com/download/download/26183/QNX_Neutrino_RTOS_System_Architecture.pdf)

115. A figure from the '698 patent is provided below, showing an exemplary embodiment where operating states are monitored by a trusted component. In this example, boot up and a re-boot via BIOS are monitored by a trusted component.



('698, Fig. 7.)

116. An illustrative description of BlackBerry's infringement on an element-by-element basis is provided below for exemplary claims of the patent.

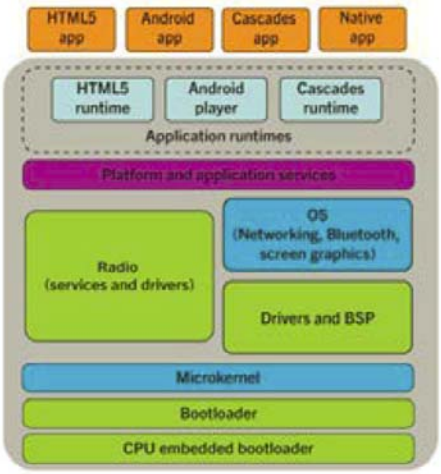
- *1[p]. A computing entity comprising:*

QNX Neutrino and associated implementations as provided by BlackBerry comprise a computing entity.

- *1[a] a computer platform comprising*

QNX Neutrino provides a computer platform for computing entities with a variety of implementations. For example, the BlackBerry 10 operating system platform

sits on the BlackBerry device entities, and BlackBerry provides a QNX Neutrino platform in other applications and implementations.



BlackBerry 10 platform

(Sources: https://global.blackberry.com/en/software; https://help.blackberry.com/en/blackberry-security-overview/latest/blackberry-security-overview/awi1402929620791.html)

> The BlackBerry 10 OS is a microkernel operating system that is based on the QNX Neutrino RTOS.

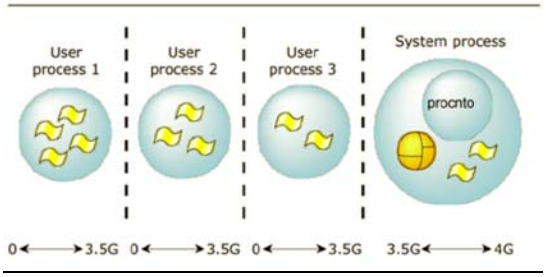
(Source: https://help.blackberry.com/en/blackberry-security-overview/latest/blackberry-security-overview/awi1402930370721.html)

- *1[b]. a plurality of physical and logical resources including a first data processor and a first memory;*

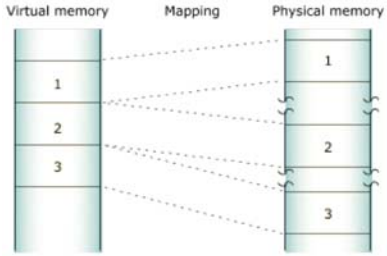
QNX Neutrino implementations include physical and logical resources including data processors and memory. For example, the BlackBerry 10 OS contains various processes, which may include a first user process with its (first) memory address space.

> The process manager is capable of creating multiple POSIX processes (each of which may contain multiple POSIX threads).
>
> In the QNX Neutrino RTOS, the microkernel is paired with the Process Manager in a single module (procnto). This module is required for all runtime systems.

(Source: http://support7.qnx.com/download/download/26183/QNX_Neutrino_RTOS_System_Architecture.pdf)



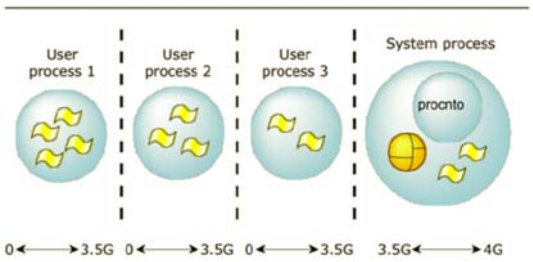
(Source:https://developer.blackberry.com/native/documentation/dev/rtos/arch/proc_memman.html)



(Source: https://developer.blackberry.com/native/documentation/dev/rtos/arch/proc_memman.html)

- *1[c]. a monitoring component comprising a second data processor and a second memory;*

QNX Neutrino, such as in the BlackBerry 10 OS and other implementations, contains a monitoring component comprising a second data processor and memory space. For example, the High Availability Manager including associated components "provides a mechanism for monitoring processes and services on your system." (Source: http://support7.qnx.com/download/ download/26183/QNX_Neutrino_RTOS_System_Architecture.pdf) The process of monitoring states (and associated memory) is separate and distinct from other data processing and memory.



(Source: https://developer.blackberry.com/native/documentation/dev/rtos/arch/proc_memman.html)

> The High Availability Manager (HAM) provides a mechanism for monitoring processes and services on your system. The goal is to provide a resilient manager (or "smart watchdog") that can perform multistage recovery whenever system services or processes fail, no longer respond, or are detected to be in a state where they cease to provide acceptable levels of service. Entities are the fundamental units of observation/monitoring in the system. Essentially, an entity is a process (pid). As processes, all entities are uniquely identifiable by their pids.

(Source: http://support7.qnx.com/download/download/26183/QNX_Neutrino_RTOS_System_Architecture.pdf)

> Create fault tolerant applications
>
> Under this system, every driver, application, protocol stack, and file system runs outside the kernel in the safety of memory-protected user space. Virtually any component can fail and be automatically restarted without affecting other components or the kernel. Further, the QNX OS provides an optional high-availability framework for ensuring critical software is monitored and kept running even after faults.

(Source: http://support7.qnx.com/download/download/26406/QNX%20OS%20Security.pdf)

> If a process stops responding, it isolates a process in its user space and restarts the process without negatively affecting other processes. It uses adaptive partitioning to prevent apps from interfering with or reading the memory used by another

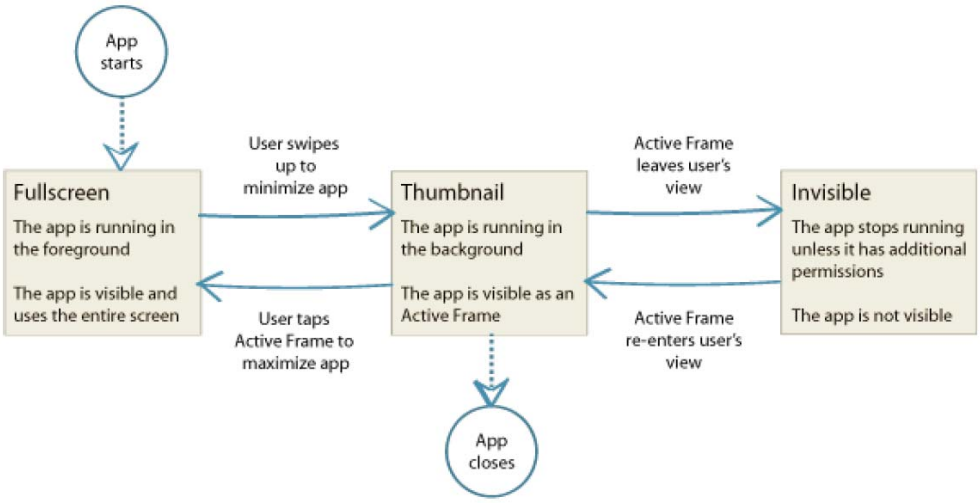
> app. It validates requests for resources and controls how apps access the capabilities of the device, such as access to the camera, contacts, and device identifying information.

(Source: https://help.blackberry.com/en/blackberry-security-overview/latest/blackberry-security-overview/awi1402930370721.html)

- *1[d]. wherein, said computer platform is capable of operating in a plurality of different states, each said state utilising a corresponding respective set of individual ones of said physical and logical resources;*

QNX Neutrino provides for different states that use different computer resources, and BlackBerry provides implementations that include multiple different states. For example, BlackBerry 10 can transition to different application processes, each process having a state and corresponding resources (e.g., their own protected address spaces). Multiple different states are monitored by High Availability Manager components. QNX Neutrino also provides different kernel states such as "running, "ready," and "blocked" that utilize different computer resources.

> An app can transition between states as a result of a user's action or because of the state of the device.
>
> …
>
> The following diagram shows how an app can move from state to state:



(Source: https://developer.blackberry.com/native/documentation/dev/states/transitions_in_app_life_cycle.html)

> With memory protection, if one of the processes executing in a multitasking environment attempts to access memory that hasn't been explicitly declared or allocated for the type of access attempted, the MMU hardware can notify the OS, which can then abort the thread (at the failing/offending instruction). This protects process address spaces from each other, preventing coding errors in a thread in one process from damaging memory used by threads in other processes or even in the OS. This protection is useful both for development and for the installed runtime system, because it makes postmortem analysis possible.

(Source: https://developer.blackberry.com/native/documentation/dev/rtos/arch/proc_memman.html)

Kernel states, the complete list

Here's the complete list of kernel blocking states, with brief explanations of each state.

By the way, this list is available in **`<sys/states.h>`**—you'll notice that the states are all prefixed with STATE_ , but the prefix tends to be omitted in conversation and the documentation (for example, "READY" is really STATE_READY):

If the state is:	The thread is:
STATE_CONDVAR	Waiting for a condition variable to be signaled
STATE_DEAD	Dead. Kernel is waiting to release the thread's resources
STATE_INTR	Waiting for an interrupt
STATE_JOIN	Waiting for the completion of another thread
STATE_MUTEX	Waiting to acquire a mutex

STATE_NANOSLEEP Sleeping for a period of time

STATE_NET_REPLY Waiting for a reply to be delivered across the network

STATE_NET_SEND Waiting for a pulse or message to be delivered across the network

STATE_READY Not running on a CPU, but is ready to run (one or more higher or equal priority threads are running)

STATE_RECEIVE Waiting for a client to send a message

STATE_REPLY Waiting for a server to reply to a message

STATE_RUNNING Actively running on a CPU

STATE_SEM Waiting to acquire a semaphore

STATE_SEND Waiting for a server to receive a message

STATE_SIGSUSPEND Waiting for a signal

STATE_SIGWAITINFO Waiting for a signal

STATE_STACK Waiting for more stack to be allocated

STATE_STOPPED Suspended (SIGSTOP signal)

STATE_WAITCTX Waiting for a register context (usually floating point) to become available (only on SMP systems)

STATE_WAITPAGE Waiting for process manager to resolve a fault on a page

STATE_WAITTHREAD Waiting for a thread to be created

(Source: http://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.neutrino.getting_started/topic/s1_procs_Kernel_states.html)

Kernel states

We've been talking about "running," "ready," and "blocked" loosely—let's now formalize these thread states.

RUNNING

QNX Neutrino's RUNNING state simply means that the thread is now actively consuming the CPU. On an SMP system, there will be multiple threads running; on a single-processor system, there will be one thread running.

READY

The READY state means that this thread *could* run right now—except that it's not, because another thread, (at the same or higher priority), is running. If two threads were capable of using the CPU, one thread at priority 10 and one thread at priority 7, the priority 10 thread would be RUNNING, and the priority 7 thread would be READY.

The blocked states

What do we call the blocked state? The problem is, there's not just *one* blocked state. Under QNX Neutrino, there are in fact over a dozen blocking states.

Why so many? Because the kernel keeps track of *why* a thread is blocked.

(Source: http://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.neutrino.getting_started/topic/s1_procs_kstate.html)

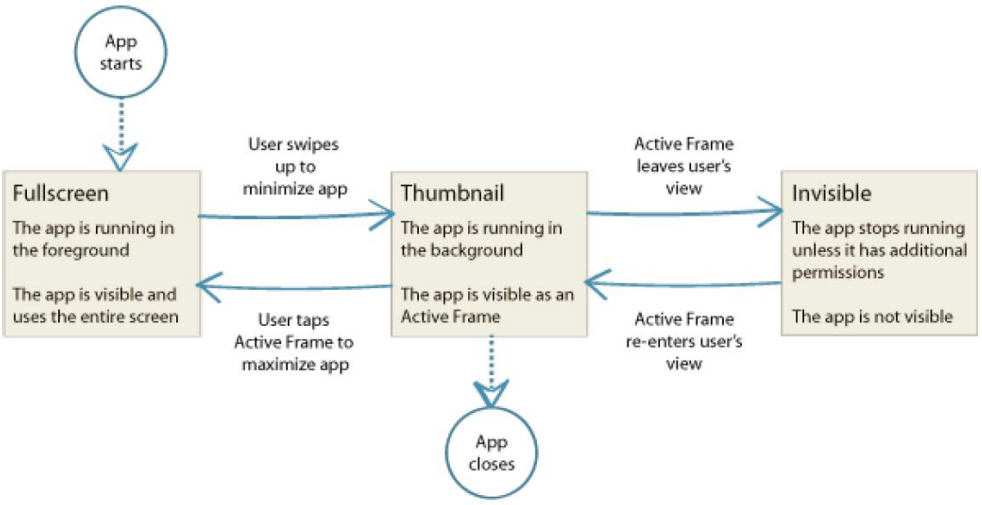
- *1[e]. wherein said monitoring component operates to determine which of said plurality of states is the current operating state of said computer platform.*

QNX Neutrino includes monitoring functionality to determine which state is the current state. For example, High Availability Manager components determine which state is the current operating state. See Claim 1[c] above. (Source: http://support7.qnx.com/download/download/26183/QNX_Neutrino_RTOS_System_Architecture.pdf)

In a BlackBerry 10 OS implementation, the monitoring component determines the current operating state.

> An app can transition between states as a result of a user's action or because of the state of the device. These transitions make up your app's life cycle. When an app makes a transition from one state of the life cycle to another, the BlackBerry 10 OS notifies the app using events. The events that an app receives can vary depending on the way the user configures the settings on the device. … The BlackBerry 10 OS can deactivate your app and move it to the background at any time. For example, a user may leave your app to open another app. When the OS deactivates your app, your code should first save the app state. In addition, your app should stop any unnecessary threads and processes (such as updating the UI in real time) to preserve system resources. When the OS activates your app again, you can reload the saved state, and restart any suspended processes.

(Source: https://developer.blackberry.com/native/documentation/dev/states/transitions_in_app_life_cycle.html)



(Source: https://developer.blackberry.com/native/documentation/dev/states/transitions_in_app_life_cycle.html)

- *3. The computing entity as claimed in claim 1, in which exit of said computer platform from each said operating state is monitored by said monitoring component.*

On information and belief, the exit of the QNX Neutrino platform from each operating state is monitored by the monitoring component.

- *20[p]. A method of storing data at a computing entity comprising a computer platform*

See claim 1[p]-[a].

- *20[a] having a first data processor and a first memory*

See claim 1[b].

- *20[b] and a monitoring component having a second data processor and a second memory, said method comprising the steps of:*

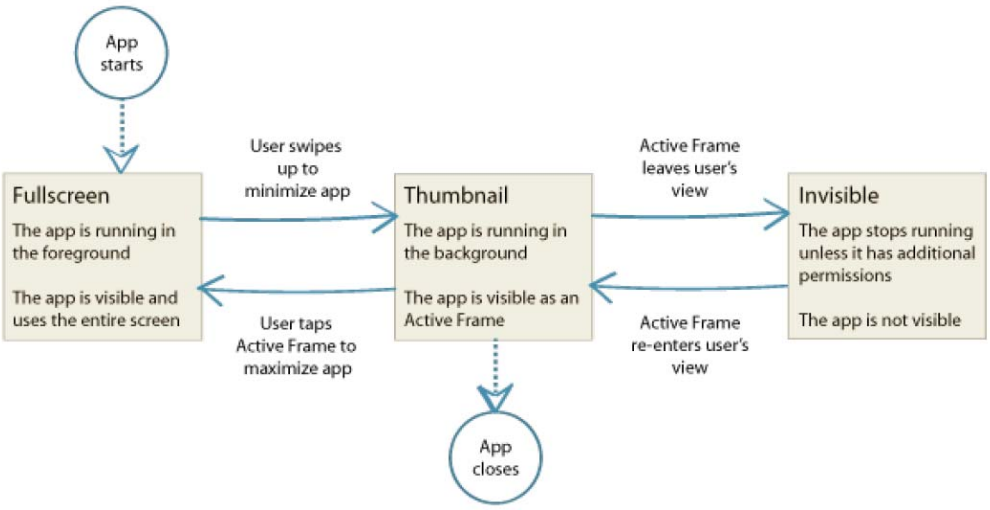
See claim 1[c].

- *20[c] initiating a session on the computing platform;*

BlackBerry's QNX Neutrino initiates a session on the computing platform. For example, a user app process or other process is started that begins a session.

> The process manager is capable of creating multiple POSIX processes (each of which may contain multiple POSIX threads).
>
> In the QNX Neutrino RTOS, the microkernel is paired with the Process Manager in a single module (procnto). This module is required for all runtime systems.

(Source: http://support7.qnx.com/download/download/26183/QNX_Neutrino_RTOS_System_Architecture.pdf)

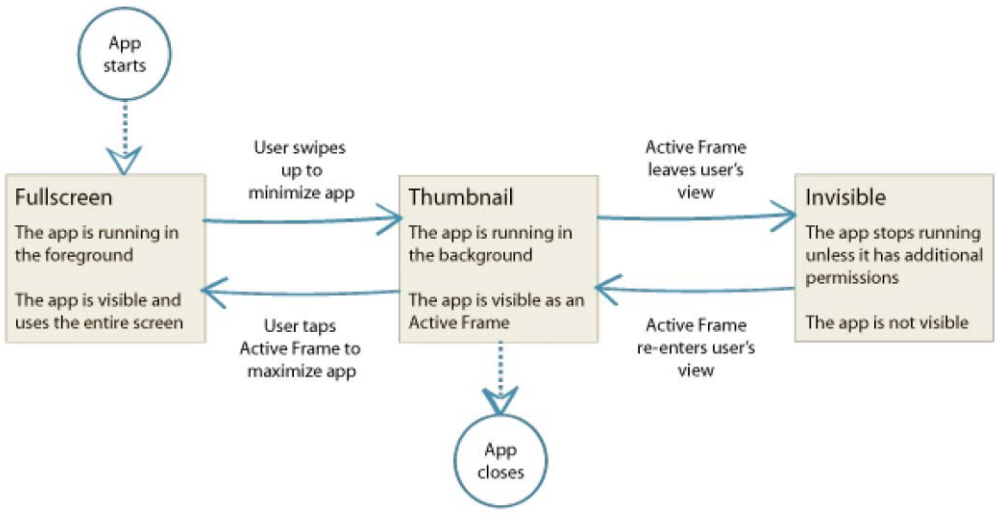


(Source: https://developer.blackberry.com/native/documentation/dev/states/transitions_in_app_life_cycle.html)

- *20[d]. the monitoring component recording state data describing a current operational state of the computing platform;*

See Claim 1[c] and 1[e] regarding the monitoring component and High Availability Manager. The monitoring component records and determines the state of processes and kernel states and records descriptive data.

> An app can transition between states as a result of a user's action or because of the state of the device. These transitions make up your app's life cycle. When an app makes a transition from one state of the life cycle to another, the BlackBerry 10 OS notifies the app using events. The events that an app receives can vary depending on the way the user configures the settings on the device.
>
> The following diagram shows how an app can move from state to state:



(Source: https://developer.blackberry.com/native/documentation/dev/states/transitions_in_app_life_cycle.html)

> The High Availability Manager (HAM) provides a mechanism for monitoring processes and services on your system. The goal is to provide a resilient manager (or "smart watchdog") that can perform multistage recovery whenever system services or processes fail, no longer respond, or are detected to be in a state where they cease to provide acceptable levels of service. Entities are the fundamental units of observation/monitoring in the system. Essentially, an entity is a process (pid). As processes, all entities are uniquely identifiable by their pids.

(Source: http://support7.qnx.com/download/download/26183/QNX_Neutrino_RTOS_System_Architecture.pdf)

- *20[e]. generating data in the session; and*

QNX Neutrino generates data in the session. For example, an app process session generates its own app data (*e.g.*, information about the state) which eventually needs to be saved, and other processes generate data during the session.

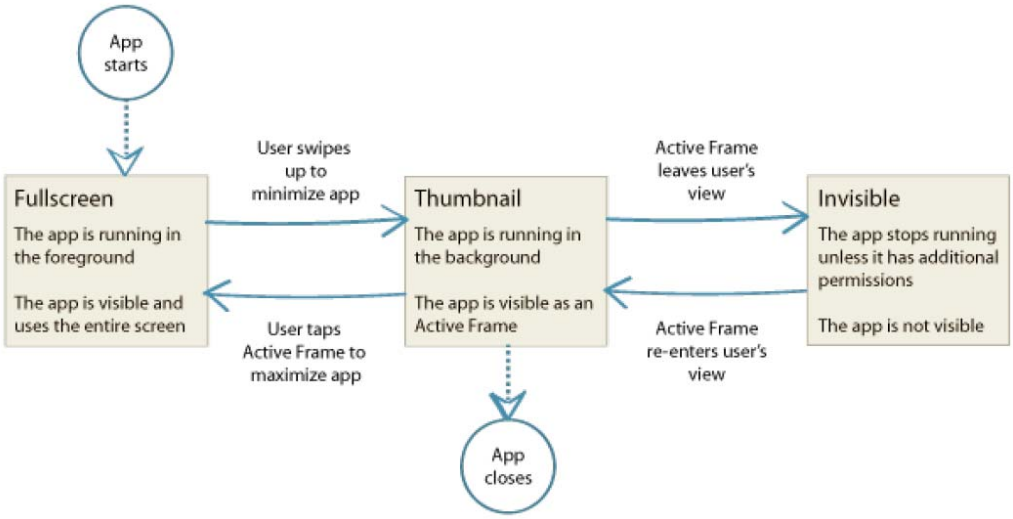
> The BlackBerry 10 OS can deactivate your app and move it to the background at any time. For example, a user may leave your app to open another app. When the OS deactivates your app, your code should first save the app state. In addition,

> your app should stop any unnecessary threads and processes (such as updating the UI in real time) to preserve system resources. When the OS activates your app again, you can reload the saved state, and restart any suspended processes.
>
> An app can also experience interruptions during its life cycle such as losing focus, low memory events, and low battery events. Your app should listen for these events and respond by saving information about the state of the app. For example, the screen element currently in focus, or any user-entered data, should be saved. The saved state can be reloaded so that when the user returns to the app, the user can then continue on as before.

(Source: https://developer.blackberry.com/native/documentation/dev/states/transitions_in_app_life_cycle.html)

- *20[f]. storing the generated data with reference to the state data so that the generated data may be recovered in a future session of the computing platform in the same operational state.*

QNX Neutrino stores the generated data with reference to the state data so that generated data may be recovered in a future session in the same operational state. For example, the data generated by an app is saved so that it may be recovered in the same state when the computing platform reactivates the app. The High Availability Manager provides "a resilient manager (or 'smart watchdog') that can perform multistage recovery whenever system services or processes fail, no longer respond, or are detected to be in a state where they cease to provide acceptable levels of service." (Source: http://support7.qnx.com/download/download/26183/QNX_Neutrino_RTOS_System_Architecture.pdf)



(Source: https://developer.blackberry.com/native/documentation/dev/states/transitions_in_app_life_cycle.html)

> The BlackBerry 10 OS can deactivate your app and move it to the background at any time. For example, a user may leave your app to open another app. When the OS deactivates your app, your code should first save the app state. In addition, your app should stop any unnecessary threads and processes (such as updating the UI in real time) to preserve system resources. When the OS activates your app again, you can reload the saved state, and restart any suspended processes.

(Source: https://developer.blackberry.com/native/documentation/dev/states/transitions_in_app_life_cycle.html)

> The High Availability Manager (HAM) provides a mechanism for monitoring processes and services on your system. The goal is to provide a resilient manager (or "smart watchdog") that can perform multistage recovery whenever system services or processes fail, no longer respond, or are detected to be in a state where they cease to provide acceptable levels of service. Entities are the fundamental units of observation/monitoring in the system. Essentially, an entity is a process (pid). As processes, all entities are uniquely identifiable by their pids.

(Source: http://support7.qnx.com/download/download/26183/QNX_Neutrino_RTOS_

System_Architecture.pdf)

117. Facebook is entitled to relief as a result of BlackBerry's infringement, including without limitation monetary damages no less than a reasonable royalty.

118. On information and belief, compliance with 35 U.S.C. § 287 has been achieved to the extent applicable to the asserted claims of the Patents-in-Suit and/or is not applicable to the asserted claims of the Patents-in-Suit.

PRAYER FOR RELIEF

WHEREFORE, Facebook respectfully requests:

A. That Judgment be entered that BlackBerry has infringed each of the Patents-in-Suit under 35 U.S.C. § 271;

B. An award of monetary damages sufficient to compensate Facebook for BlackBerry's infringement under 35 U.S.C. § 284;

C. Costs and expenses incurred by Facebook in this action;

D. An award of prejudgment and post-judgment interest; and

E. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Facebook respectfully demands a trial by jury on all issues triable by jury.

Dated: September 4, 2018

COOLEY LLP

/s/ *Heidi L. Keefe*
Heidi L. Keefe (178960)

HEIDI L. KEEFE (178960)
(hkeefe@cooley.com)
MARK R. WEINSTEIN (193043)
(mweinstein@cooley.com)
MATTHEW J. BRIGHAM (191428)
(mbrigham@cooley.com)
LOWELL D. MEAD (223989)
(lmead@cooley.com)
3175 Hanover Street
Palo Alto, CA 94304-1130
Telephone: (650) 843-5000
Facsimile: (650) 849-7400

COOLEY LLP
MICHAEL G. RHODES (116127)
(rhodesmg@cooley.com)
101 California Street
5th Floor
San Francisco, CA 94111-5800
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

Attorneys for Plaintiff
FACEBOOK, INC.