EXHIBIT 5

APPLE 1101

HBCU TECHNOLOGY FOUNDATION'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 11,653,183 – Apple Inc.

Claims 20 and 30

HBCU Technology Foundation ("HBCU") provides evidence of infringement of claim 1 of U.S. Patent No. 11,653,183 (hereinafter "the ' 183 patent") by Apple Inc. ("Apple"). In support thereof, HBCU provides the following claim charts.

"Accused Instrumentalities" as used herein is defined in HBCU's Complaint. It is further understood, on information an belief, that Apple retains ownership of all relevant Apple-provided software on user's Apple devices, and that such software is responsible, in material part, for the functionality of those devices.

These claim charts demonstrate Apple's infringement, and provide notice of such infringement, by comparing each element of the asserted claims to corresponding components, aspects, and/or features of the Accused Instrumentalities. These claim charts are not intended to constitute an expert report on infringement. These claim charts include information provided by way of example, and not by way of limitation.

The analysis set forth below is based only upon information from available resources regarding the Accused Instrumentalities, as Apple has not yet provided any further non-public information. The analysis also takes into account the Certificate of Correction issued on July 9, 2024, as reflected below. An analysis of Apple's (or other third parties') technical documentation and/or software source code may assist in fully identifying all infringing features and functionality. Accordingly, HBCU reserves the right to supplement this infringement analysis once such information is made available to HBCU. Furthermore, HBCU reserves the right to revise this infringement analysis, as appropriate, upon issuance of a court order construing any terms recited in the asserted claims. HBCU provides this evidence of infringement and related analysis without the benefit of claim construction or expert reports or discovery. HBCU reserves the right to supplement, amend or otherwise modify this analysis and/or evidence based on any such claim construction or expert reports or discovery.

Unless otherwise noted, HBCU contends that Apple directly infringes the '183 patent in violation of 35 U.S.C. § 271(a) by selling, offering to sell, making, using, and/or importing the Accused Instrumentalities. The following exemplary analysis demonstrates that infringement. Unless otherwise noted, HBCU further contends that the evidence below supports a finding of indirect infringement under 35 U.S.C. §§ 271(b) and/or (c), in conjunction with other evidence of liability under one or more of those subsections. Apple makes, uses, sells, imports, or offers for sale in the United States, or has made, used, sold, imported, or offered for sale in the past, without authority, or induces others to make, use, sell, import, or offer for sale in the United States, or has induced others to make, use, sell, import, or offer for sale in the past, without authority products, equipment, or services that infringe at least claim 1 of the '183 patent, including without limitation, the Accused Instrumentalities.

HBCU TECHNOLOGY FOUNDATION'S FIRST INFRINGEMENT ANALYSIS

Unless otherwise noted, HBCU believes and contends that each element of each claim asserted herein is literally met through Apple's provision of the Accused Instrumentalities. However, to the extent that Apple attempts to allege that any asserted claim element is not literally met, HBCU believes and contends that such elements are met under the doctrine of equivalents. More specifically, in its investigation and analysis of the Accused Instrumentalities, HBCU did not identify any substantial differences between the elements of the patent claims and the corresponding features of the Accused Instrumentalities, as set forth herein. In each instance, the identified feature of the Accused Instrumentalities performs at least substantially the same function in substantially the same way to achieve substantially the same result as the corresponding claim element.

To the extent the chart of an asserted claim relies on evidence about certain specifically identified Accused Instrumentalities, HBCU asserts that, on information and belief, any similarly functioning instrumentalities also infringes the charted claim. HBCU reserves the right to amend this infringement analysis based on other products made, used, sold, imported, or offered for sale by Apple. HBCU also reserves the right to amend this infringement analysis by citing other claims of the '183 patent, not listed in the claim chart, that are infringed by the Accused Instrumentalities. HBCU further reserves the right to amend this infringement analysis by adding, subtracting, or otherwise modifying content in the "Accused Instrumentalities" column of each chart.

Claim 1	Accused Instrumentalities
1. A system comprising:	The Accused Instrumentalities include the Apple iMessage system.
a sending mobile phone that transmits short message service (SMS) messages via a cellular network and packet switched messages via a packet switched message service (PSMS);	The Accused Instrumentalities transmit short message service (SMS) messages via a cellular network and packet switched messages via a packet switched message service (PSMS). ***The Accused Instrumentalities include a sending mobile phone that transmits SMS messages.*** Specifically, the iMessage system on the Apple iPhone sends SMS messages to non-Apple devices.

What is the difference between iMessage and SMS/MMS?

Learn why some of your message bubbles are blue or green.

You can use the Messages app on your iPhone, iPad, or iPod touch to send messages. Those messages are sent as iMessage or SMS/MMS. Learn more about the difference between the message types.

iMessage

iMessages are texts, photos, or videos that you send to another iPhone, iPad, iPod touch, or Mac over Wi-Fi or cellular-data networks. These messages are always encrypted and appear in blue text bubbles. To turn iMessage on or off, go to Settings > Messages.

SMS/MMS

If you aren't using iMessage, you can use SMS/MMS. These messages are texts and photos that you send to other cell phones or another iPhone, iPad, or iPod touch. SMS/MMS messages aren't encrypted and appear in green text bubbles on your device.

See: Exhibit 16, What is the difference between iMessage and SMS/MMS?

4

5	[T]he iMessage system provides for messages to be sent and received between devices in packet-switched form via the Internet, i.e., WLAN or WPAN, or alternatively via SMS. See: Exhibit 17, Apple Brief, dated 6/15/22, at 5. ***The Accused Instrumentalities send SMS messages via a cellular network.*** In particular, the iPhone transmits SMS messsages to non-subscribers using, for example, a 3G, 4G long term evolution (LTE) cellular network or 5G New Radio (NR) network. Exemplary 3G functionality is set forth below: 3GPP TS 23.040 V8.6.0 (2009-09) *Technical Specification* **3rd Generation Partnership Project;** **Technical Specification Group Core Network and Terminals;** **Technical realization of the Short Message Service (SMS)** **(Release 8)**

10.2 Short message mobile originated

The entities involved in this procedure is depicted in figure 17.

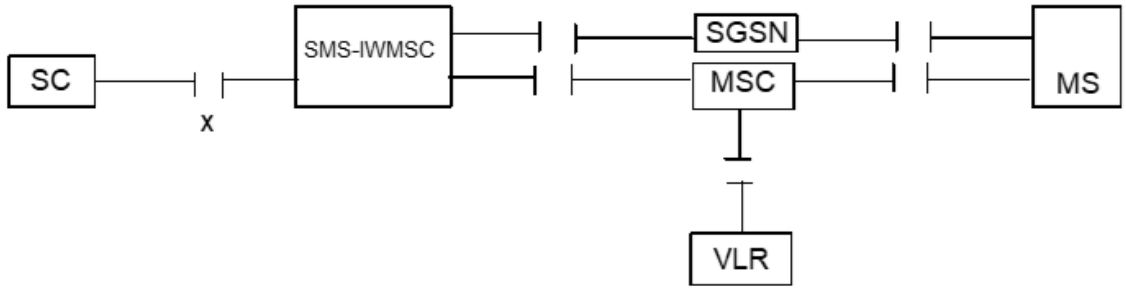


Figure 17: Interfaces involved in the Short message mobile originated procedure

See: Exhibit 23, 3GPP TS 23.040 V8.6.0 (2009-09), at 10.2

The Accused Instrumentalities include a sending mobile phone that transmits packet switched messages via a packet switched message service (PSMS).

Specifically, the iMessage system on the Apple iPhone sends non-SMS based packet switched messages (sometimes referred to "iMessages") to other Apple iPhones that appear in blue bubbles on the iPhone device. These non-SMS messages are sent over Wi-Fi or cellular data networks, making them packet switched messages. Apple's iMessage service is a service for receiving packet-switched messages.

What is the difference between iMessage and SMS/MMS?

Learn why some of your message bubbles are blue or green.

You can use the Messages app on your iPhone, iPad, or iPod touch to send messages. Those messages are sent as iMessage or SMS/MMS. Learn more about the difference between the message types.

iMessage

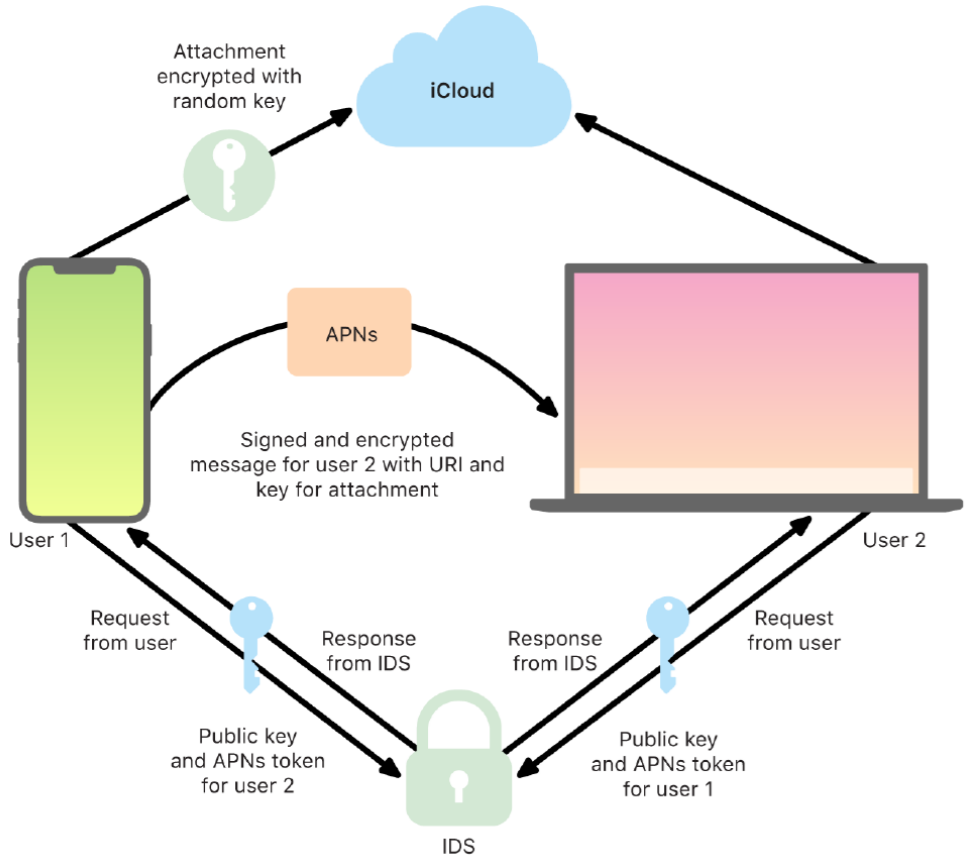
iMessages are texts, photos, or videos that you send to another iPhone, iPad, iPod touch, or Mac over Wi-Fi or cellular-data networks. These messages are always encrypted and appear in blue text bubbles. To turn iMessage on or off, go to Settings > Messages.

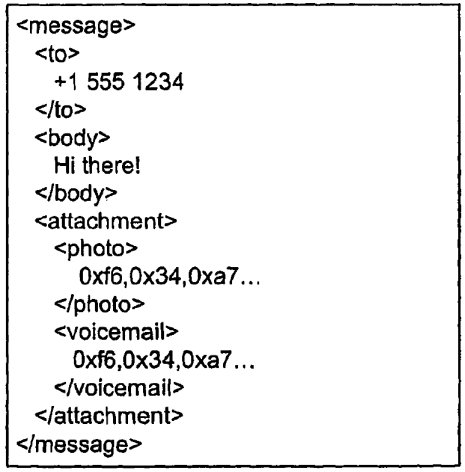
SMS/MMS

If you aren't using iMessage, you can use SMS/MMS. These messages are texts and photos that you send to other cell phones or another iPhone, iPad, or iPod touch. SMS/MMS messages aren't encrypted and appear in green text bubbles on your device.

See: Exhibit 16, What is the difference between iMessage and SMS/MMS?

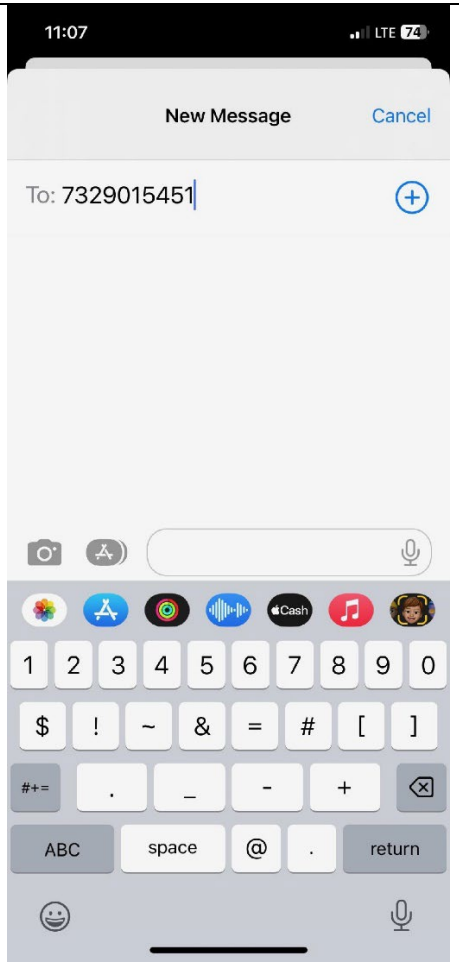
	[T]he iMessage system provides for messages to be sent and received between devices in packet-switched form via the Internet, i.e., WLAN or WPAN, or alternatively via SMS. See: Exhibit 17, Apple Brief, dated 6/15/22, at 5.
and a server that supports the PSMS;	The Accused Instrumentalities include a server that supports the PSMS. ***The Apple Identity Service (IDS) includes a server that supports the iMessage PSMS.*** In particular, the Apple Identity Service (IDS) includes a server that receives requests and provides responses to the Accused Instrumentalities and thus supports the iMessage PSMS. The IDS [Apple Identity Service] … is a database, which stores and manages the registration of Apple devices for altogether different services. For example, the database contains information about whether devices have been activated for using the iMessage service. … [T]he task of the IDS is to manage and provide registration information for a number of services, e.g. including for "FaceTime", "Handoff", "HomeKit", "Continuity", "Finding Friends", "Maps", "Digital Touch" or for the synchronization of messages. … See: Apple Rejoinder, dated 11/02/16, at 13. **How iMessage sends and receives messages securely** Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the Apple Identity Service (IDS) to retrieve the public keys and APNs addresses for all of the devices associated with the addressee. See: Exhibit 19, Apple Platform Security – May 2024, at 197. **Request for public keys at the IDS database** When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the

6	IDS database in this regard. See: Exhibit 17, Apple Brief, dated 6/15/22, at 6.  See: Exhibit 19, Apple Platform Security – May 2024, at 198.

wherein: the sending mobile phone retrieves first information representing a phone number of a first receiving mobile phone from a first message and sends the first information to the server;	The Accused Instrumentalities retrieve first information representing a phone number of a first receiving mobile phone from a first message and send the first information to the server. ***The sending mobile phone retrieves first information representing a phone number of a first receiving mobile phone from a first message.*** The patent specification describes that the message includes the destination phone number. Figure 6B, for example, demonstrates this teaching: **FIG. 6B**  *See also* '183 patent at 5:48. The specification describes other examples. *See, e.g., id.* at 7:9-41. The Accused Instrumentalities operate in the same manner. Specifically, when composing a new message for a new conversation, the user of the sending mobile phone can enter either a phone number or email address into the address field of the message. In cases where the user of the sending mobile phone enters a phone number into the address field, first information representing a phone number of a first receiving mobile phone is retrieved from a first message.

	How iMessage sends and receives messages securely Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the Apple Identity Service (IDS) to retrieve the public keys and APNs addresses for all of the devices associated with the addressee. See: Exhibit 19, Apple Platform Security – May 2024, at 197. **Request for public keys at the IDS database** When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the IDS database in this regard. See: Exhibit 17, Apple Brief, dated 6/15/22, at 6.

11



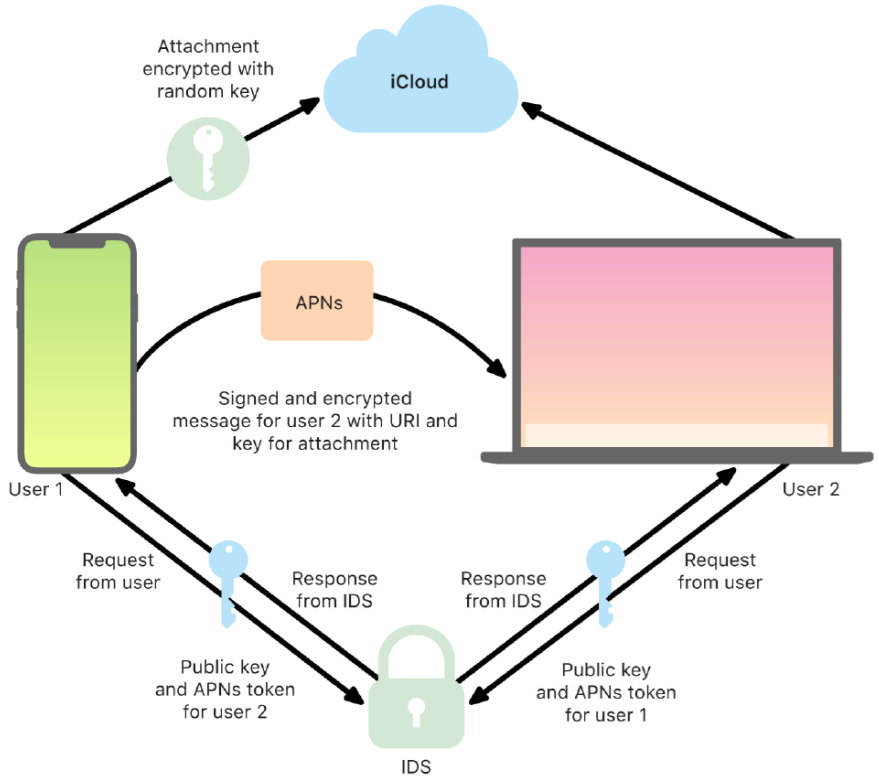
See: Exhibit 20, Apple iPhone Screenshot taken August 26, 2024.

The sending mobile phone sends the first information to the server.

As noted above, the Apple IDS comprises the "server" that supports the iMessage PSMS. The sending mobile phone sends a request message that includes information representative of the phone number of the first receiving mobile phone to the IDS. While, in the diagram from the Apple Security Guide,

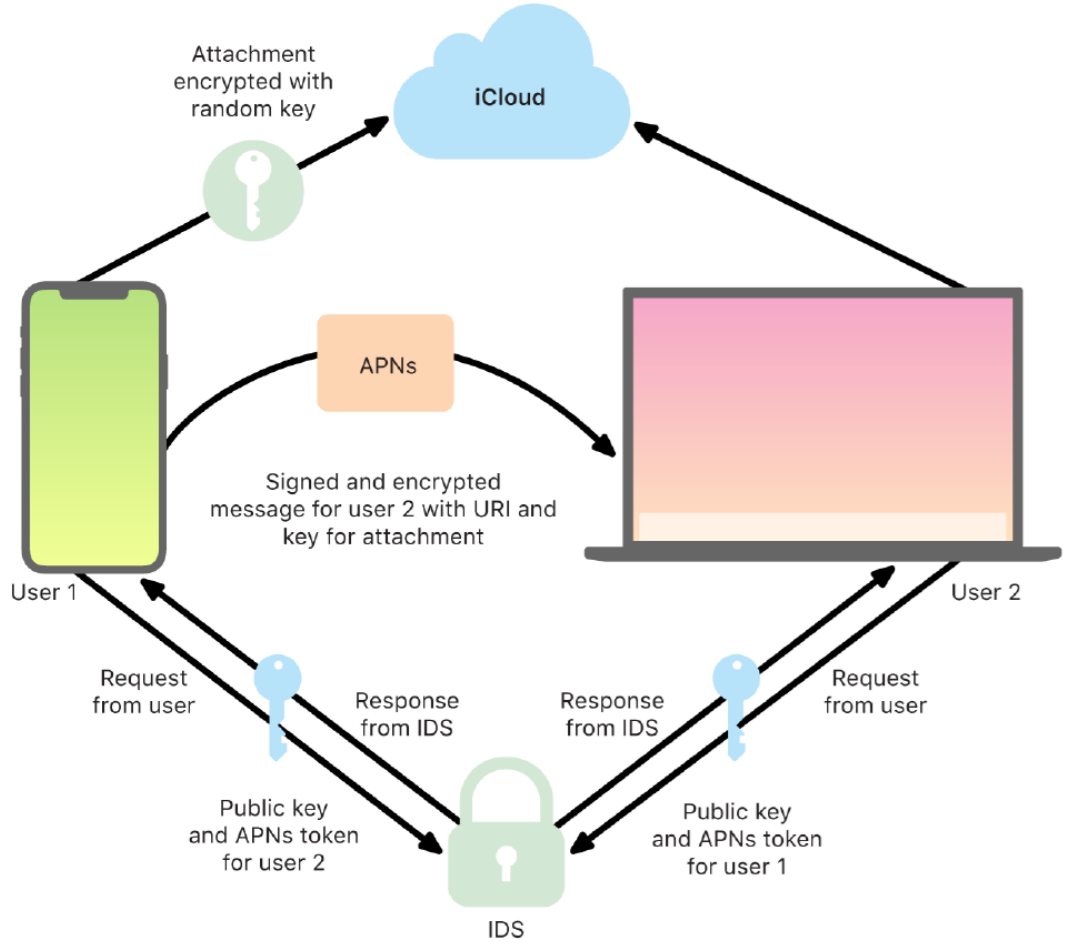
	shown below, User 2 corresponds to a laptop, the iMessage system uses the same request/response messages in a case where User 2 corresponds to a receiving mobile phone. **How iMessage sends and receives messages securely** Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the Apple Identity Service (IDS) to retrieve the public keys and APNs addresses for all of the devices associated with the addressee. See: Exhibit 19, Apple Platform Security – May 2024, at 197. **Request for public keys at the IDS database** When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the IDS database in this regard. See: Exhibit 17, Apple Brief, dated 6/15/22, at 6.

13

	 See: Exhibit 19, Apple Platform Security – May 2024, at 198.
the server, in response to receipt of the first information, sends a first response to the sending mobile phone when the phone number of the first receiving mobile phone is not associated with a subscriber of the PSMS;	In response to receipt of the first information, the Accused Instrumentalities send a first response to the sending mobile phone when the phone number of the first receiving mobile phone is not associated with a subscriber of the PSMS. ***The server, in response to receipt of the first information, sends a first response to the sending mobile phone when the phone number of the first receiving mobile phone is not associated with a subscriber of the PSMS.***

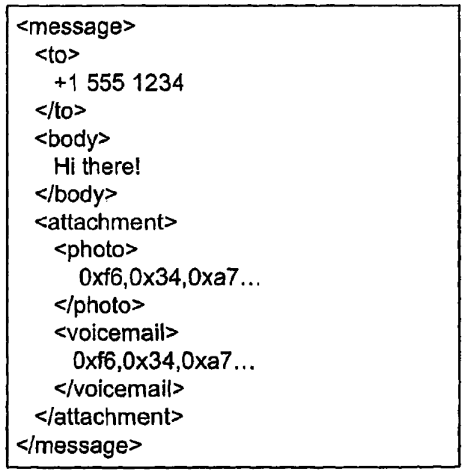
	As noted above, the Apple IDS comprises the "server," and the sending mobile phone sends a request message that includes information representative of the phone number of the first receiving mobile phone to the IDS. When the phone number of the first receiving mobile phone is not associated with a subscriber of the PSMS (e.g., a registered iMessage user) in the IDS, the IDS sends a "first response" which lacks public keys. 1. Request for public keys at the IDS database When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the IDS database in this regard. a) Public keys are stored in the IDS database if ● the receiving device is registered for iMessage and … See: Exhibit 17, Apple Brief, dated June 15, 2022, at 5, 6. The sending mobile wireless device registered with iMessage decides to send the messages to the receiving device as SMS instead of iMessage if it does not receive public keys in response to the request to the IDS database for the receiving device. ... If public keys are received/available for the receiving device, the sending device basically sends the message via iMessage. Apple Brief, dated 6/15/22, at 5-6.

15



See: Exhibit 19, Apple Platform Security – May 2024, at 198.

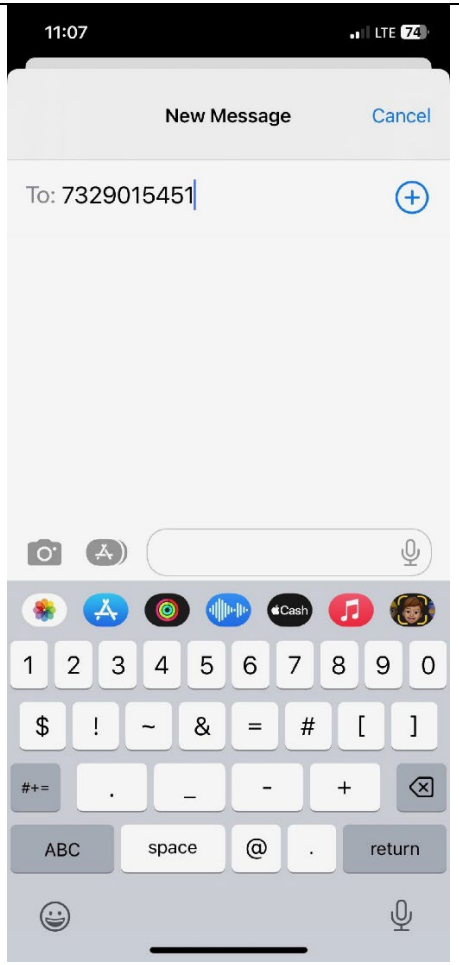
after the first response is received by the sending mobile phone, the sending mobile phone sends the first message via an SMS bearer to the first receiving mobile phone;	After the first response is received by the sending mobile phone, the Accused Instrumentalities send the first message via an SMS bearer to the first receiving mobile phone. ***After the first response is received by the sending mobile phone, the sending mobile phone sends the first message via an SMS bearer to the first receiving mobile phone.*** In particular, after the sending iPhone fails to receive keys in the first response, the sending iPhone transmits the message to the first receiving mobile phone via an SMS bearer. > The sending mobile wireless device registered with iMessage decides to send the messages to the receiving device as SMS instead of iMessage if it does not receive public keys in response to the request to the IDS database for the receiving device. See: Exhibit 17, Apple Brief, dated June 15, 2022, at 5, 6 > [T]he confirmation of verification communicated to the sending device ... is the basis for the decision of the sending device: if it is negative, the message is sent via SMS bearer, if it is positive, the message can basically be sent as iMessage and thus via packet-switched bearer. See: Exhibit 17, Apple Brief dated 6/15/22, at 5.
the sending mobile phone retrieves second information representing a phone number of a second receiving mobile phone from a second message being composed and sends the second information to the server; the second receiving mobile phone being	The Accused Instrumentalities retrieve second information representing a phone number of a second receiving mobile phone from a second message being composed and send the second information to the server. ***The sending mobile phone retrieves second information representing a phone number of a second receiving mobile phone from a second message being composed.*** The patent specification describes that the message includes the destination phone number. Figure 6B, for example, demonstrates this teaching:

associated with a subscriber of the PSMS;	FIG. 6B  *See also* '183 patent at 5:48. The specification describes other examples. *See, e.g., id.* at 7:9-41. The Accused Instrumentalities operate in the same manner. Specifically, when composing a new message for a new conversation, the user of the sending mobile phone can enter either a phone number or email address into the address field of the message. In cases where the user of the sending mobile phone enters a phone number into the address field, second information representing a phone number of a second receiving mobile phone is retrieved from a second message being composed. **How iMessage sends and receives messages securely** Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the Apple Identity Service (IDS) to retrieve the public keys and APNs addresses for all of the devices associated with the addressee.

18

	See: Exhibit 19, Apple Platform Security – May 2024, at 197. **Request for public keys at the IDS database** When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the IDS database in this regard. See: Exhibit 17, Apple Brief, dated 6/15/22, at 6.

19



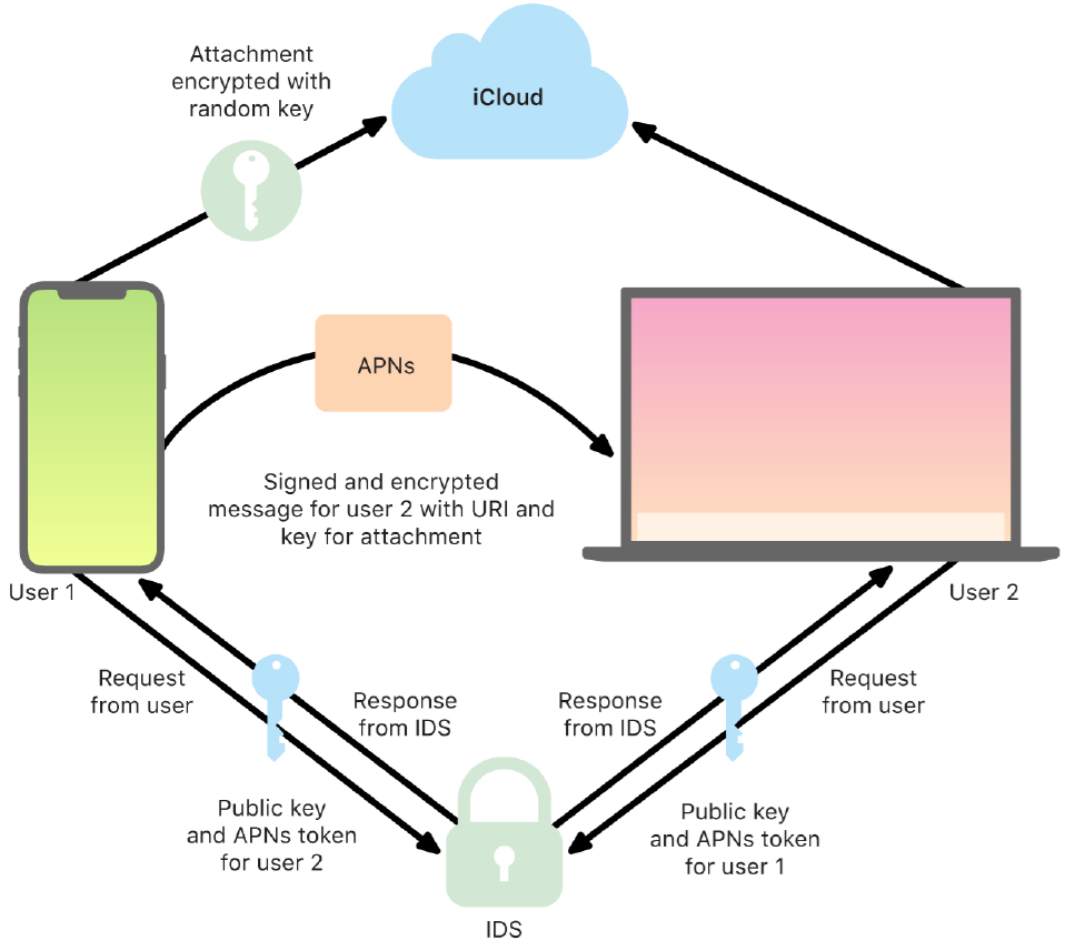
See: Exhibit 20, Apple iPhone Screenshot taken August 26, 2024.

The sending mobile phone sends the second information to the server.

As noted above, the Apple IDS comprises the "server" that supports the iMessage PSMS. The sending mobile phone sends a second request message that includes information representative of the phone

20

	number of the second receiving mobile phone to the IDS. While in the diagram from the Apple Security Guide shown above User 2 corresponds to a laptop, the iMessage system uses the same request/response messages in a case where User 2 corresponds to a receiving mobile phone. **How iMessage sends and receives messages securely** Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the Apple Identity Service (IDS) to retrieve the public keys and APNs addresses for all of the devices associated with the addressee. See: Exhibit 19, Apple Platform Security – May 2024, at 197. **Request for public keys at the IDS database** When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the IDS database in this regard. See: Exhibit 17, Apple Brief, dated 6/15/22, at 6.

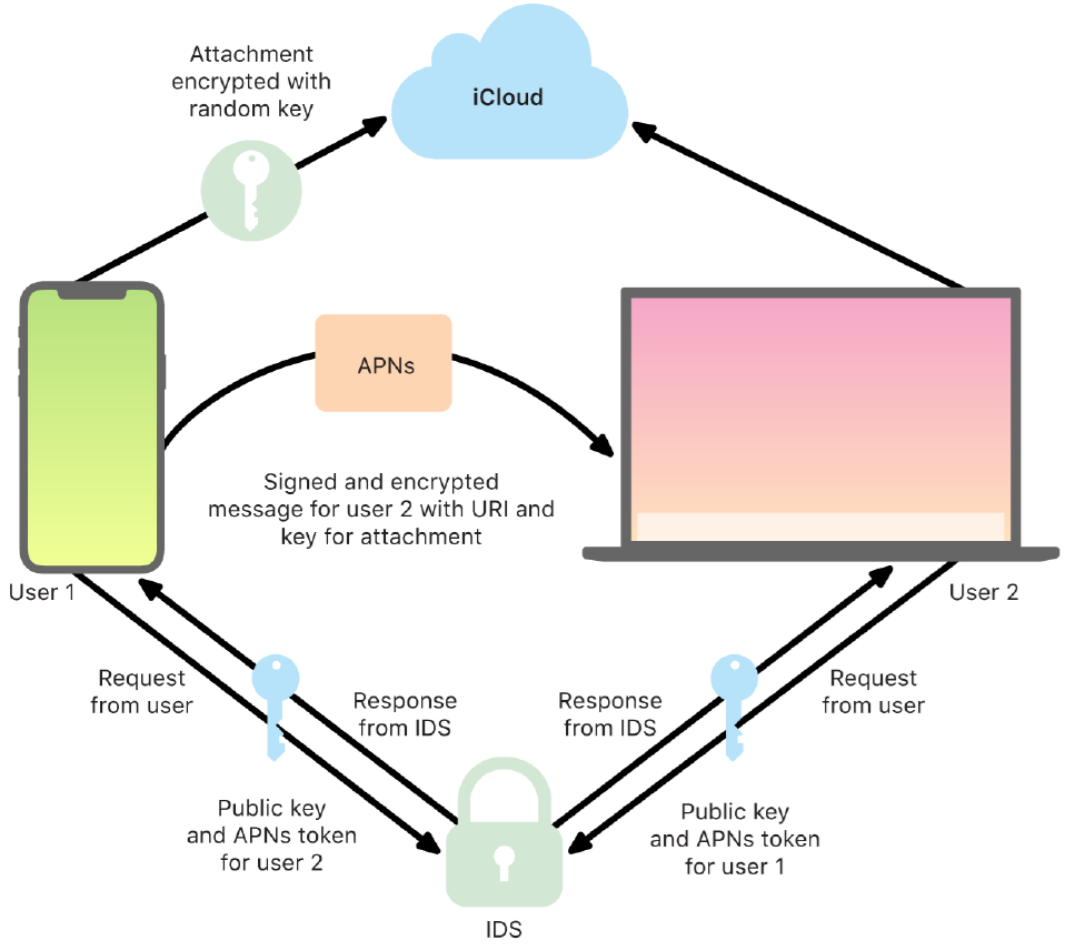


See: Exhibit 19, Apple Platform Security – May 2024, at 198.

22

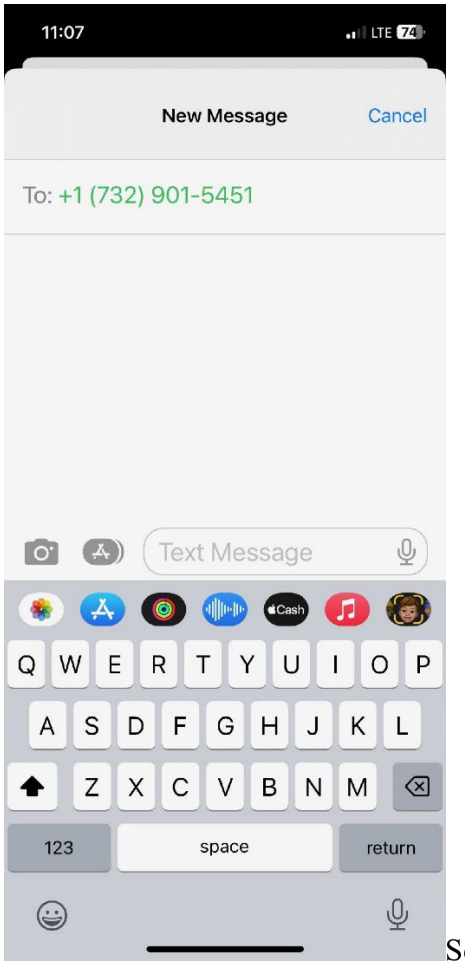
	The Accused Instrumentalities include a second receiving mobile phone being associated with a subscriber of the PSMS. ***The second receiving mobile phone is associated with a subscriber of the PSMS.*** As noted above, the Apple IDS comprises the "server," and the sending mobile phone sends a request message that includes information representative of the phone number of the second receiving mobile phone to the IDS. The second receiving mobile phone corresponds to a registered iMessage user ("a subscriber of the PSMS"). **How iMessage sends and receives messages securely** Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the Apple Identity Service (IDS) to retrieve the public keys and APNs addresses for all of the devices associated with the addressee. See: Exhibit 19, Apple Platform Security – May 2024, at 197. **Request for public keys at the IDS database** When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the IDS database in this regard. See: Exhibit 17, Apple Brief, dated 6/15/22, at 6. The sending mobile wireless device registered with iMessage decides to send the messages to the receiving device as SMS instead of iMessage if it does not receive public keys in response to the request to the IDS database for the receiving device. ... If public keys are received/available for the receiving device, the sending device basically sends the message via iMessage. Apple Brief, dated 6/15/22, at 5-6.

the server, in response to receipt of the second information, sends a second response to the sending mobile phone, the second response communicating a different query result than the first response;	In response to receipt of the second information, the Accused Instrumentalities send a second response to the sending mobile phone, the second response communicating a different query result than the first response. ***The server, in response to receipt of the second information, sends a second response to the sending mobile phone, the second response communicating a different query result than the first response.*** As noted above, the Apple IDS comprises the "server," and the sending mobile phone sends a request message that includes information representative of the phone number of the second receiving mobile phone to the IDS. The IDS responds to this request message with a "second response." In a case where the second response includes encryption keys associated with the second receiving mobile phone (assoicated with an iMessage subscriber), the second response communicates a different query result than the first response (which lacked encryption keys). 1. Request for public keys at the IDS database When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the IDS database in this regard. a) Public keys are stored in the IDS database if ● the receiving device is registered for iMessage and … See: Exhibit 17, Apple Brief, dated June 15, 2022, at 5, 6. The sending mobile wireless device registered with iMessage decides to send the messages to the receiving device as SMS instead of iMessage if it does not receive public keys in response to the request to the IDS database for the receiving device. ... If public keys are received/available for the receiving device, the sending device basically sends the message via iMessage. Apple Brief, dated 6/15/22, at 5-6.

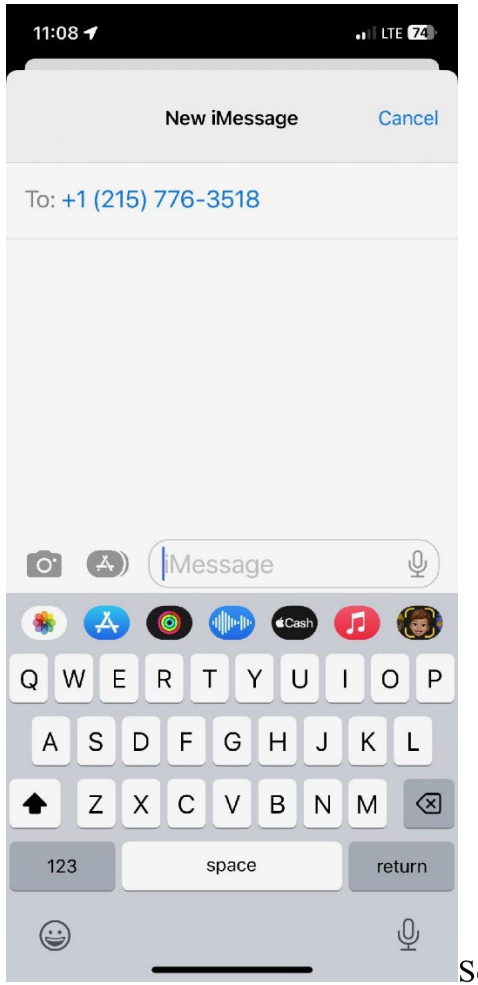


See: Exhibit 19, Apple Platform Security – May 2024, at 198.

This is further demonstrated by the actions taken in each instance, as further set forth below.



See: Exhibit 20, Apple iPhone Screenshot taken August 26, 2024.



See: Exhibit 20, Apple iPhone Screenshot taken August 26, 2024.

27

the sending mobile phone sends the second message via a wireless local area network (WLAN) and via the PSMS, to the second receiving mobile phone on a condition that a maximum number of undelivered messages corresponding to the second receiving mobile phone has not been exceeded;	The Accused Instrumentalities send the second message via a wireless local area network (WLAN) and via the PSMS, to the second receiving mobile phone on a condition that a maximum number of undelivered messages corresponding to the second receiving mobile phone has not been exceeded. ***The sending mobile phone sends the second message via the PSMS to the second receiving mobile phone.*** Specifically, the iPhone selects the iMessage service ("the PSMS") for transmission of the second message based at least in part on the IDS indicating that the addressed recipient corresponds to a subscriber of the service by returning encryption keys for the addressed recipient. **1. Request for public keys at the IDS database** When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the IDS database in this regard. a) Public keys are stored in the IDS database if ● the receiving device is registered for iMessage and … Apple Brief, dated 6/15/22, at 5-6. The sending mobile wireless device registered with iMessage decides to send the messages to the receiving device as SMS instead of iMessage if it does not receive public keys in response to the request to the IDS database for the receiving device. ... If public keys are received/available for the receiving device, the sending device basically sends the message via iMessage. Apple Brief, dated 6/15/22, at 5-6. ***The sending mobile phone sends the second message via a WLAN to the second receiving mobile phone.*** Specifically, in at least some cases where WiFi is available, the iPhone sends the second message using the iMessage service ("the PSMS") via a Wi-Fi wireless local area network (WLAN).

iMessages are texts, photos, or videos that you send to another iPhone, iPad, iPod touch, or Mac over Wi-Fi or cellular-data networks. These messages are always encrypted and appear in blue text bubbles. To turn iMessage on or off, go to Settings > Messages.

If you aren't using iMessage, you can use SMS/MMS. These messages are texts and photos that you send to other cell phones or another iPhone, iPad, or iPod touch. SMS/MMS messages aren't encrypted and appear in green text bubbles on your device.

To use SMS/MMS on an iPhone, you need a text-messaging plan. Contact your wireless carrier for more information. You can also set up your other Apple devices to send and receive messages from any Apple device.

If Wi-Fi is unavailable, iMessages will be sent over cellular data. Cellular data rates might apply.

See: Exhibit 16, What is the difference between iMessage and SMS/MMS?

29

Wi-Fi specifications for Apple devices

The following are Wi-Fi specification details for Apple devices. Descriptions of the details are as follows:

- *802.11 compatibility and frequency band:* 802.11ax (Wi-Fi 6 and Wi-Fi 6E), 802.11ac (Wi-Fi 5), 802.11n (Wi-Fi 4), 802.11a, 802.11b/g and 2.4 GHz or 5 GHz.

  Apple platforms supporting Wi-Fi 6E can join Wi-Fi 6E networks that are discoverable on 2.4 GHz or 5 GHz channels, and on 6 GHz Preferred Scanning Channels, where 6 GHz is allowed by regulatory domain.

See: Wi-Fi specifications for Apple devices - Apple Support.

The sending mobile phone sends the second message on a condition that a maximum number of undelivered messages corresponding to the second receiving mobile phone has not been exceeded.

In particular, in cases where the sending iPhone fails to receive delivery confirmation(s) for a threshold number of one or more previous iMessages sent to the second mobile receiving device, the sending iPhone sends the second message to the second mobile receiving device via SMS. The "maximum number of underlivered messages" corresponds to the threshold number of one or more previous iMessages for which no delivery confirmation was received. So long as the threshold number of undelivered messages is not exceeded, the sending mobile phone sends the second message via the PSMS after the IDS returns encryption keys for the second receiving mobile phone.

> In addition, the sending device takes into account the "history" of its – and only its - previous communication with the receiving device. Within the iMessage system, the receiving mobile wireless device sends an acknowledgement message to the sending device when it has received the message. The sending device registers when it has sent a message and has not received a verification message from the receiving device within a predetermined time. If this has happened several times in a row, when it sends a new message to this destination address, it decides not to send it as an iMessage and thus packet-switched, even if it receives the public keys (which Plaintiff considers as a confirmatory response to the verification request), but sends it by SMS bearer.

	… If public keys are received/available for the receiving device, the sending device basically sends the message via iMessage. An exception and a dispatch via SMS takes place if it has sent messages via iMessage to the receiving device in the past for which it has not received any acknowledgement messages from the receiving device and then changes the transmission path based on this local available information due to the assumption that the recipient cannot be reached via iMessage. See: Exhibit 17, Apple Brief, dated 6/15/22, at 4-6
the PSMS is a service for sending and receiving packet switched messages other than SMS, enhanced message service (EMS) and multimedia message service (MMS) messages; and	The Accused Instrumentalities include a PSMS, which is a service for sending and receiving packet switched messages other than SMS, enhanced message service (EMS) and multimedia message service (MMS) messages. ***The PSMS is a service for sending and receiving packet switched messages other than SMS, enhanced message service (EMS) and multimedia message service (MMS) messages.*** Specifically, Apple's iMessage service is a packet switched message service ("PSMS") for sending and receiving packet-switched messages (such as iMessages) other than SMS, EMS or MMS messages. [T]he iMessage system provides for messages to be sent and received between devices in packet-switched form via the Internet, i.e., WLAN or WPAN, or alternatively via SMS. See: Exhibit 17, Apple Brief, dated 6/15/22, at 5.

What is the difference between iMessage and SMS/MMS?

Learn why some of your message bubbles are blue or green.

You can use the Messages app on your iPhone, iPad, or iPod touch to send messages. Those messages are sent as iMessage or SMS/MMS. Learn more about the difference between the message types.

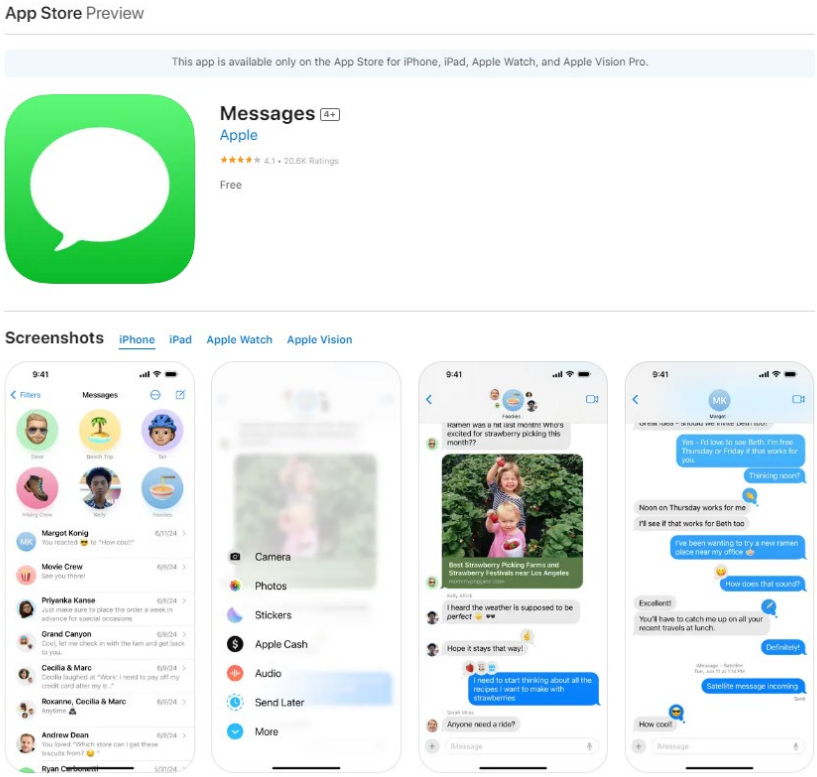
iMessage

iMessages are texts, photos, or videos that you send to another iPhone, iPad, iPod touch, or Mac over Wi-Fi or cellular-data networks. These messages are always encrypted and appear in blue text bubbles. To turn iMessage on or off, go to Settings > Messages.

SMS/MMS

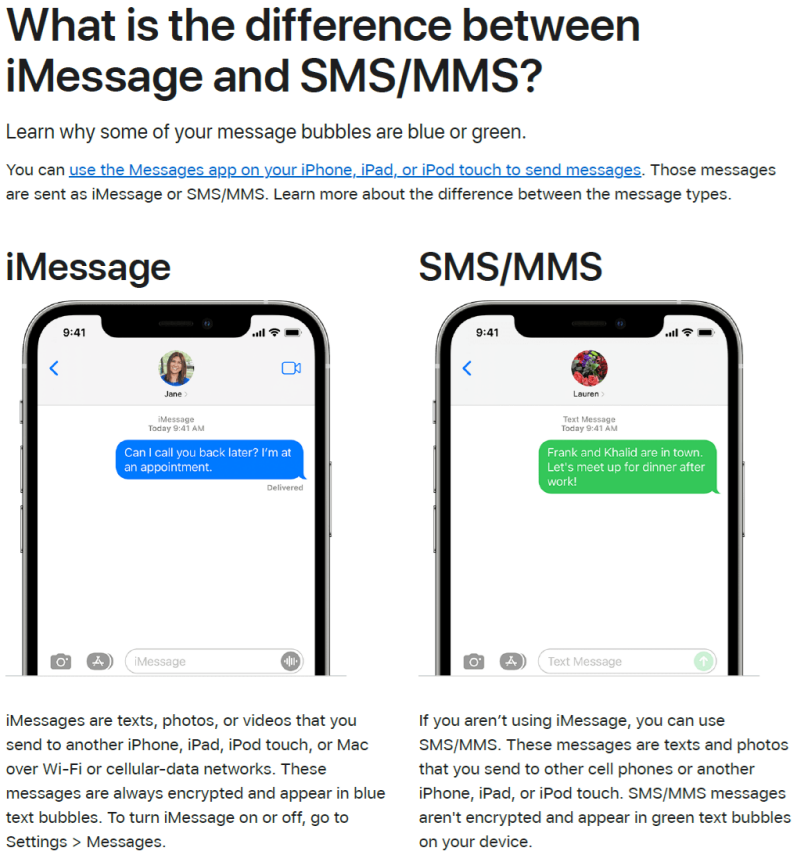
If you aren't using iMessage, you can use SMS/MMS. These messages are texts and photos that you send to other cell phones or another iPhone, iPad, or iPod touch. SMS/MMS messages aren't encrypted and appear in green text bubbles on your device.

See: Exhibit 16, What is the difference between iMessage and SMS/MMS?

content of the first message and content of the second message is displayed by a same messaging client.	In Accused Instrumentalities, the SMS message sent to the first receiving mobile phone and the message sent to the second receiving mobile phone are originated via a same messaging client. ***The iPhone includes a messaging client.*** In particular, the Apple "Messages App" comprises a messaging client.  See: Apple Store Preview (http://apps.apple.com/us/app/messages/id1146560473)

The content of the first message sent (via SMS) to the first receiving mobile phone and the content of the second message sent (via the PSMS) to the second receiving mobile phone are originated via a same messaging client.

Specifically, the Apple "Messages App" on the iPhone includes a common messaging client that displays the content of both SMS messages (including the "first message") and packet-switched messages (including "the second message") sent using the iMessage service.



See: Exhibit 16, What is the difference between iMessage and SMS/MMS?

20. A method performed by a sending mobile phone that transmits short message service (SMS) messages via a cellular network and packet switched messages via a packet switched message service (PSMS), the method comprising:	The Accused Instrumentalities transmits short message service (SMS) messages via a cellular network and packet switched messages via a packet switched message service (PSMS). ***The Accused Instrumentalities include a sending mobile phone that transmits SMS messages.*** Specifically, the iMessage system on the Apple iPhone sends SMS messages to non-Apple devices.

35

What is the difference between iMessage and SMS/MMS?

Learn why some of your message bubbles are blue or green.

You can use the Messages app on your iPhone, iPad, or iPod touch to send messages. Those messages are sent as iMessage or SMS/MMS. Learn more about the difference between the message types.

iMessage

iMessages are texts, photos, or videos that you send to another iPhone, iPad, iPod touch, or Mac over Wi-Fi or cellular-data networks. These messages are always encrypted and appear in blue text bubbles. To turn iMessage on or off, go to Settings > Messages.

SMS/MMS

If you aren't using iMessage, you can use SMS/MMS. These messages are texts and photos that you send to other cell phones or another iPhone, iPad, or iPod touch. SMS/MMS messages aren't encrypted and appear in green text bubbles on your device.

See: Exhibit 16, What is the difference between iMessage and SMS/MMS?

	[T]he iMessage system provides for messages to be sent and received between devices in packet-switched form via the Internet, i.e., WLAN or WPAN, or alternatively via SMS. See: Exhibit 17, Apple Brief, dated 6/15/22, at 5. ***The Accused Instrumentalities send SMS messages via a cellular network.*** In particular, the iPhone transmits SMS messsages to non-subscribers using a 4G long term evolution (LTE) cellular network or 5G New Radio (NR) network. ***The Accused Instrumentalities include a sending mobile phone that transmits packet switched messages via a packet switched message service (PSMS).*** Specifically, the iMessage system on the Apple iPhone sends non-SMS based packet switched messages (sometimes referred to "iMessages") to other Apple iPhones that appear in blue bubbles on the iPhone device. These non-SMS messages are sent over Wi-Fi or cellular data networks, making them packet switched messages. Apple's iMessage service is a service for receiving packet-switched messages.

What is the difference between iMessage and SMS/MMS?

Learn why some of your message bubbles are blue or green.

You can use the Messages app on your iPhone, iPad, or iPod touch to send messages. Those messages are sent as iMessage or SMS/MMS. Learn more about the difference between the message types.

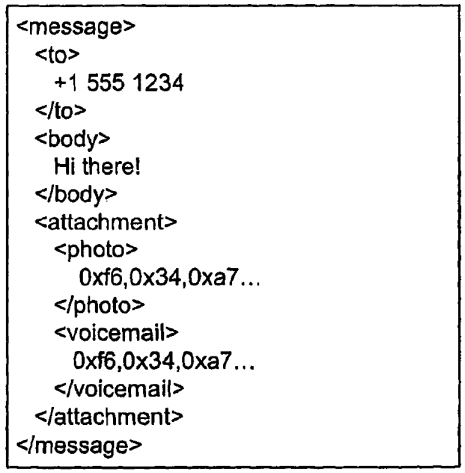
iMessage

iMessages are texts, photos, or videos that you send to another iPhone, iPad, iPod touch, or Mac over Wi-Fi or cellular-data networks. These messages are always encrypted and appear in blue text bubbles. To turn iMessage on or off, go to Settings > Messages.

SMS/MMS

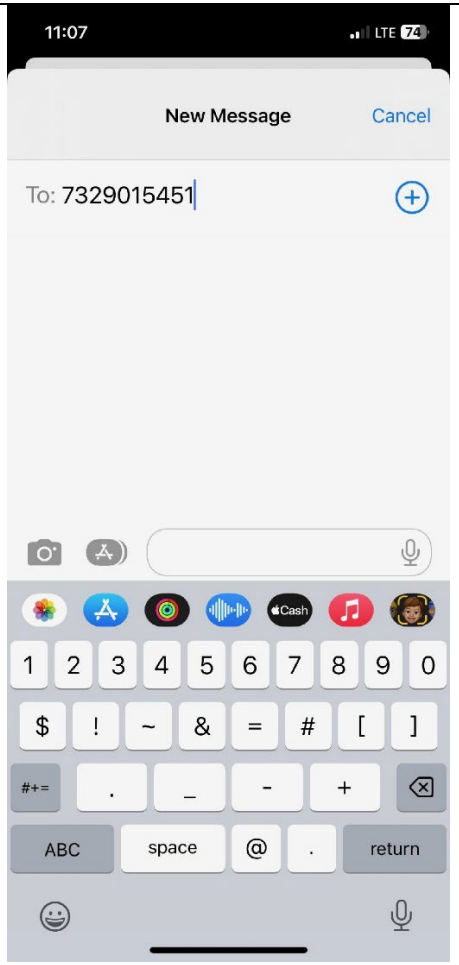
If you aren't using iMessage, you can use SMS/MMS. These messages are texts and photos that you send to other cell phones or another iPhone, iPad, or iPod touch. SMS/MMS messages aren't encrypted and appear in green text bubbles on your device.

See: Exhibit 16, What is the difference between iMessage and SMS/MMS?

retrieving, by the sending mobile phone, a phone number of a receiving mobile phone from a first message being composed and sending first information representing the phone number of the receiving mobile phone;	The Accused Instrumentalities retrieve first information representing a phone number of a first receiving mobile phone from a first message and send the first information to the server. ***The sending mobile phone retrieves a phone number of a first receiving mobile phone from a first message being composed.*** The patent specification describes that the message includes the destination phone number. Figure 6B, for example, demonstrates this teaching: **FIG. 6B**  *See also* '183 patent at 5:48. The specification describes other examples. *See, e.g., id.* at 7:9-41. The Accused Instrumentalities operate in the same manner. Specifically, when composing a new message for a new conversation, the user of the sending mobile phone can enter either a phone number or email address into the address field of the message. In cases where the user of the sending mobile phone enters a phone number into the address field, information representing a phone number of a first receiving mobile phone is retrieved from a first message.

	How iMessage sends and receives messages securely Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the Apple Identity Service (IDS) to retrieve the public keys and APNs addresses for all of the devices associated with the addressee. See: Exhibit 19, Apple Platform Security – May 2024, at 197. **Request for public keys at the IDS database** When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the IDS database in this regard. See: Exhibit 17, Apple Brief, dated 6/15/22, at 6.

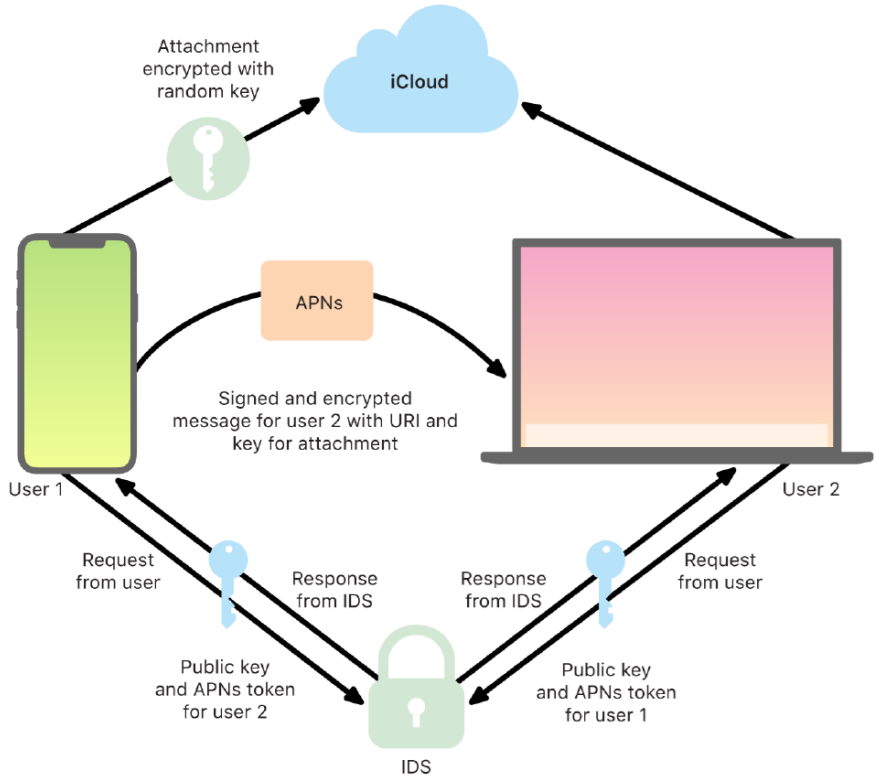
40



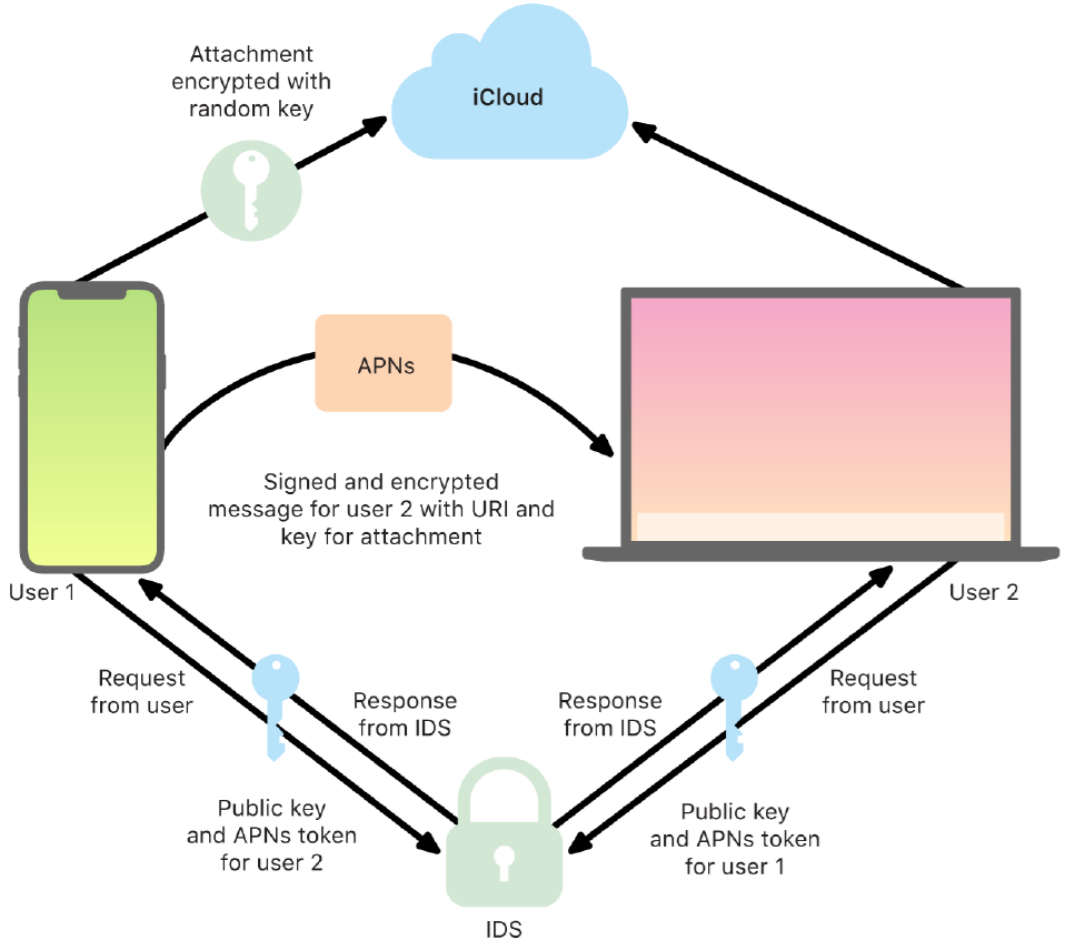
See: Exhibit 20, Apple iPhone Screenshot taken August 26, 2024.

The sending mobile phone sends the first information representing the phone number of the receiving mobile phone.

	Specifically, the sending mobile phone sends a request message that includes information representative of the phone number of the first receiving mobile phone to the Apple Identity Service (IDS). While, in the diagram from the Apple Security Guide, shown below, User 2 corresponds to a laptop, the iMessage system uses the same request/response messages in a case where User 2 corresponds to a receiving mobile phone. **How iMessage sends and receives messages securely** Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the Apple Identity Service (IDS) to retrieve the public keys and APNs addresses for all of the devices associated with the addressee. See: Exhibit 19, Apple Platform Security – May 2024, at 197. **Request for public keys at the IDS database** When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the IDS database in this regard. See: Exhibit 17, Apple Brief, dated 6/15/22, at 6.

	 See: Exhibit 19, Apple Platform Security – May 2024, at 198.
receiving, by the sending mobile phone, a first response to the sending, wherein the first response indicates that the receiving mobile phone is associated with a subscriber of the PSMS;	In response to receipt of the first information, the Accused Instrumentalities send a first response to the sending mobile phone when the phone number of the first receiving mobile phone is not associated with a subscriber of the PSMS. ***The sending mobile phone receives a first response to the sending, wherein the first response indicates that the receiving mobile phone is associated with a subscriber of the PSMS.*** As noted above, the sending mobile phone sends a request message that includes information representative of the phone number of the receiving mobile phone to the IDS. The IDS responds to this request message with a "first response" which is received "by the sending mobile phone." In a case

	where the first response includes encryption keys associated with the receiving mobile phone, the response indicates that the receiving mobile phone is associated with a subscriber of the PSMS. 1. Request for public keys at the IDS database When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the IDS database in this regard. a) Public keys are stored in the IDS database if ● the receiving device is registered for iMessage and … See: Exhibit 17, Apple Brief, dated June 15, 2022, at 5, 6. The sending mobile wireless device registered with iMessage decides to send the messages to the receiving device as SMS instead of iMessage if it does not receive public keys in response to the request to the IDS database for the receiving device. ... If public keys are received/available for the receiving device, the sending device basically sends the message via iMessage. Apple Brief, dated 6/15/22, at 5-6.

	 See: Exhibit 19, Apple Platform Security – May 2024, at 198.
after the first response is received by the sending mobile phone, sending, by the sending mobile phone, the first message	After the first response is received by the sending mobile phone, the Accused Instrumentalities send, by the sending mobile phone, the first message via a wireless local area network (WLAN) and the PSMS. ***The sending mobile phone sends the first message via the PSMS.***

via a wireless local area network (WLAN) and the PSMS; and	Specifically, the iPhone selects the iMessage service ("the PSMS") for transmission of the first message based at least in part on the IDS indicating that the addressed recipient corresponds to a subscriber of the service by returning encryption keys for the addressed recipient. **1. Request for public keys at the IDS database** When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database by sending a request to the IDS database in this regard. a) Public keys are stored in the IDS database if ● the receiving device is registered for iMessage and … Apple Brief, dated 6/15/22, at 5-6. The sending mobile wireless device registered with iMessage decides to send the messages to the receiving device as SMS instead of iMessage if it does not receive public keys in response to the request to the IDS database for the receiving device. ... If public keys are received/available for the receiving device, the sending device basically sends the message via iMessage. Apple Brief, dated 6/15/22, at 5-6. ***The sending mobile phone sends the first message via a WLAN.*** Specifically, in at least some cases where WiFi is available, the iPhone sends the first message using the iMessage service ("the PSMS") via a Wi-Fi wireless local area network (WLAN).

47

iMessages are texts, photos, or videos that you send to another iPhone, iPad, iPod touch, or Mac over Wi-Fi or cellular-data networks. These messages are always encrypted and appear in blue text bubbles. To turn iMessage on or off, go to Settings > Messages.

If you aren't using iMessage, you can use SMS/MMS. These messages are texts and photos that you send to other cell phones or another iPhone, iPad, or iPod touch. SMS/MMS messages aren't encrypted and appear in green text bubbles on your device.

To use SMS/MMS on an iPhone, you need a text-messaging plan. Contact your wireless carrier for more information. You can also set up your other Apple devices to send and receive messages from any Apple device.

If Wi-Fi is unavailable, iMessages will be sent over cellular data. Cellular data rates might apply.

See: Exhibit 16, What is the difference between iMessage and SMS/MMS?

	Wi-Fi specifications for Apple devices The following are Wi-Fi specification details for Apple devices. Descriptions of the details are as follows: • *802.11 compatibility and frequency band:* 802.11ax (Wi-Fi 6 and Wi-Fi 6E), 802.11ac (Wi-Fi 5), 802.11n (Wi-Fi 4), 802.11a, 802.11b/g and 2.4 GHz or 5 GHz. Apple platforms supporting Wi-Fi 6E can join Wi-Fi 6E networks that are discoverable on 2.4 GHz or 5 GHz channels, and on 6 GHz Preferred Scanning Channels, where 6 GHz is allowed by regulatory domain. See: Wi-Fi specifications for Apple devices - Apple Support.
sending, by the sending mobile phone, a second message via an SMS bearer, to the receiving mobile phone, subsequent to the sending mobile phone receiving the first response and based at least in part on the first message being undelivered to the receiving mobile phone;	The Accused Instrumentalities perform, sending, by the sending mobile phone, a second message via an SMS bearer, to the receiving mobile phone, subsequent to the sending mobile phone receiving the first response and based at least in part on the first message being undelivered to the receiving mobile phone. ***Sending, by the sending mobile phone, a second message via an SMS bearer, to the receiving mobile phone, subsequent to the sending mobile phone receiving the first response and based at least in part on the first message being undelivered to the receiving mobile phone.*** In particular, in cases where the sending iPhone fails to receive delivery confirmation(s) for a threshold number of one or more previous iMessages (including "the first message") sent to the receiving mobile phone, the sending iPhone sends a subsequent message ("a second message") to receiving mobile phone via SMS. The selection of an SMS bearer for the second message is based at least in part on the first message being undelivered to the receiving mobile phone. In addition, the sending device takes into account the "history" of its – and only its - previous communication with the receiving device. Within the iMessage system, the receiving mobile wireless device sends an acknowledgement message to the sending device when it has received the message. The sending device registers when it has sent a message

48

	and has not received a verification message from the receiving device within a predetermined time. If this has happened several times in a row, when it sends a new message to this destination address, it decides not to send it as an iMessage and thus packet-switched, even if it receives the public keys (which Plaintiff considers as a confirmatory response to the verification request), but sends it by SMS bearer. This consideration of pending acknowledgement messages for the receipt of previous messages by the sending device takes place outside and independently of the verification ... … If public keys are received/available for the receiving device, the sending device basically sends the message via iMessage. An exception and a dispatch via SMS takes place if it has sent messages via iMessage to the receiving device in the past for which it has not received any acknowledgement messages from the receiving device and then changes the transmission path based on this local available information due to the assumption that the recipient cannot be reached via iMessage. See: Exhibit 17, Apple Brief, dated 6/15/22, at 4-6.
wherein the PSMS is a service for sending and receiving packet switched messages other than SMS, enhanced message service (EMS) and multimedia message service (MMS) messages.	The Accused Instrumentalities include a PSMS, which is a service for sending and receiving packet switched messages other than SMS, enhanced message service (EMS) and multimedia message service (MMS) messages. ***The PSMS is a service for sending and receiving packet switched messages other than SMS, enhanced message service (EMS) and multimedia message service (MMS) messages.*** Specifically, Apple's iMessage service is a packet switched message service for sending and receiving packet-switched messages (e.g., iMessages) which are other than SMS, EMS and MMS messages. [T]he iMessage system provides for messages to be sent and received between devices in packet-switched form via the Internet, i.e., WLAN or WPAN, or alternatively via SMS. See: Exhibit 17, Apple Brief, dated 6/15/22, at 5.

What is the difference between iMessage and SMS/MMS?

Learn why some of your message bubbles are blue or green.

You can use the Messages app on your iPhone, iPad, or iPod touch to send messages. Those messages are sent as iMessage or SMS/MMS. Learn more about the difference between the message types.

iMessage

iMessages are texts, photos, or videos that you send to another iPhone, iPad, iPod touch, or Mac over Wi-Fi or cellular-data networks. These messages are always encrypted and appear in blue text bubbles. To turn iMessage on or off, go to Settings > Messages.

SMS/MMS

If you aren't using iMessage, you can use SMS/MMS. These messages are texts and photos that you send to other cell phones or another iPhone, iPad, or iPod touch. SMS/MMS messages aren't encrypted and appear in green text bubbles on your device.

See: Exhibit 16, What is the difference between iMessage and SMS/MMS?

50

30. The method of claim 20, wherein during the entire time between when the phone number of the receiving mobile phone is retrieved and when the first response is received, the receiving mobile phone is not connected to any message server.	The Accused Instrumentatlities perform, during the entire time between when the phone number of the receiving mobile phone is retrieved and when the first response is received, the receiving mobile phone is not connected to any message server. ***During the entire time between when the phone number of the receiving mobile phone is retrieved and when the first response is received, the receiving mobile phone is not connected to any message server.*** Apple maintains status information for an iPhone based on whether the iPhone sent a timely "heartbeat." The IDS will not return encryption keys for an iMessage subscriber that has missed a "heartbeat." In a case where the receiving mobile phone has gone offline (and is therefore not connected to Apple's Push Notification server(s)) but has not yet missed sending a "heartbeat" (because, e.g., the time for sending the next heartbeat has not been reached), the receiving mobile phone will retain an active status even though it is offline. In such a case, the IDS will send encryption keys (the first response) to the sending iPhone for the receiving mobile phone even though the receiving mobile phone was offline during the time between when the phone number of the retrieving mobile phone was retrieved and when the first response was received. 1. Request for public keys at the IDS database When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database… a) Public keys are stored in the IDS database if: • the receiving device is registered for iMessage and not logged out; and • the receiving device sends system messages (so-called heartbeats) to the IDS database. These heartbeats must be sent to the IDS database by each device registered with iMessage at increasing intervals. ... . See: Exhibit 17, Apple Brief, dated June 15, 2022, at 5.

	The sending mobile wireless device registered with iMessage decides to send the messages to the receiving device as SMS instead of iMessage if it does not receive public keys in response to the request to the IDS database for the receiving device. ... If public keys are received/available for the receiving device, the sending device basically sends the message via iMessage. Apple Brief, dated 6/15/22, at 5-6.

52