

EXHIBIT 7

HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 11,991,601 – Apple Inc.

Claim 26

HBCU Messaging US, LP (“HBCU”) provides evidence of infringement of claim 1 of U.S. Patent No. 11,991,601 (hereinafter “the ’601 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. 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 ’601 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 25 of the ’601 patent, including without limitation, the Accused Instrumentalities.

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

HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

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 ’601 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 25	Accused Instrumentalities
25. A system comprising:	The Accused Instrumentalities include the iMessage devices, iMessage server side components and Apple provided wireless base stations.
a base station; and	The Accused Instrumentalities include Wi-Fi base stations. <i>A base station.</i> Apple sells traditional Wi-Fi base stations. Apple also sells iPhones which operate as Wi-Fi base stations or “personal hotspots.” These personal hotspots offer Wi-Fi connectivity to devices which do not have cellular capabilities.

		
Smart Home Accessories Linksys Velop AX4200 WiFi 6 Mesh System \$249.95	Smart Home Accessories AmplifiFi Alien Router and MeshPoint Range Extender \$699.95	Smart Home Accessories AmplifiFi Alien Router \$379.95

Exhibit 24, Mesh Wi-Fi Networking, pg. 1.

How to set up a Personal Hotspot on your iPhone or iPad

A Personal Hotspot lets you share the cellular data connection of your iPhone or iPad (Wi-Fi + Cellular) when you don't have access to a Wi-Fi network.

	Set up Personal Hotspot 1. Go to Settings > Cellular > Personal Hotspot or Settings > Personal Hotspot. 2. Tap the slider next to Allow Others to Join. If you don't see the option for Personal Hotspot, contact your carrier to make sure that you can use Personal Hotspot with your plan. Connect to Personal Hotspot with Wi-Fi, Bluetooth, or USB You can connect to a Personal Hotspot using Wi-Fi, Bluetooth, or USB. And with iOS 13 or later, devices that are connected to a Personal Hotspot will stay connected, even if the screen is locked, so those devices will still get notifications and messages. When you connect a device to your Personal Hotspot, the status bar turns blue and shows how many devices have joined. The number of devices that can join your Personal Hotspot at one time depends on your carrier and iPhone model. If other devices have joined your Personal Hotspot using Wi-Fi, you can use only cellular data to connect to the internet from the host device. Use these steps to connect: Exhibit 25, How to set up a personal hotspot, pg. 1. To the extent that Apple sold the wireless router, or the Apple device is being used as a Wi-Fi hotspot, Apple’s is a direct infringer of this claim. If the wireless router is not provided by Apple, or the Apple device is not being used as a Wi-Fi hotspot, Apple is a contributory infringer as set forth in the body of the Complaint.
--	--

HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

a server system that:

The Accused Instrumentalities include a server system.

A server system.

The Apple IDS and APNs are servers of a server system.

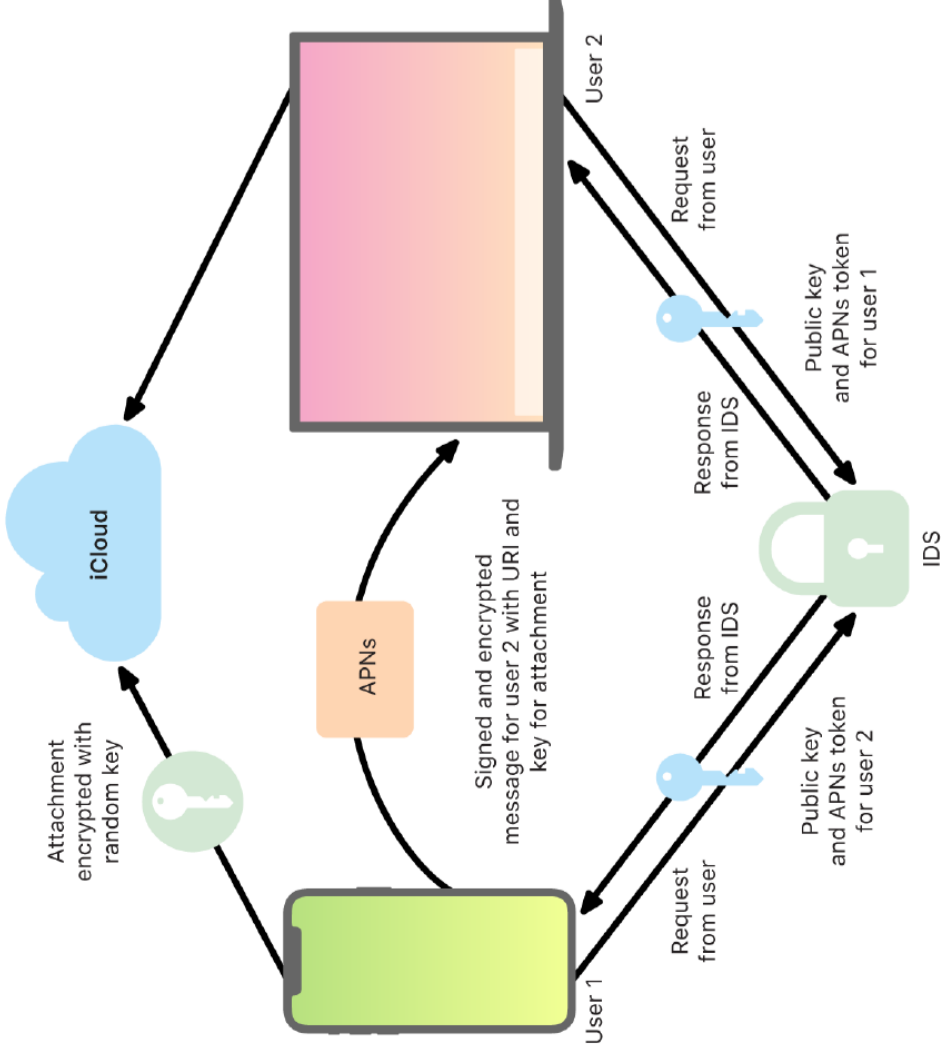


Exhibit 19, Apple Platform Security – May 2024, at 198.

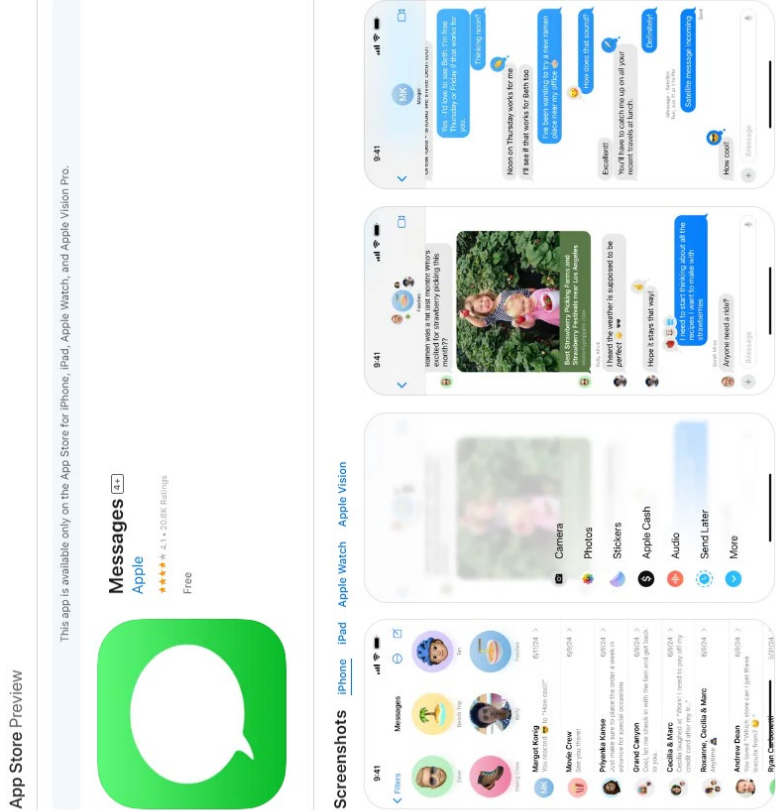
HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

receives a subscription message, from a first mobile wireless device having a message client, the subscription message indicating that the first mobile wireless device is the subscription message indicating that the first mobile wireless device is subscribing to a service for sending and receiving messages other than Short Message Service (SMS) messages, Enhanced Messaging Service (EMS) messages and Multimedia Messaging Service (MMS) messages;

The Accused Instrumentalities receive a subscription message, from a first mobile wireless device having a message client, the subscription message indicating that the first mobile wireless device is subscribing to a service for sending and receiving messages other than Short Message Service (SMS) messages, Enhanced Messaging Service (EMS) messages and Multimedia Messaging Service (MMS) messages.

The iPhone includes a messaging client.

In particular, the Apple “Messages App” comprises a messaging client.



Apple Store Preview (<http://apps.apple.com/us/app/messages/id1146560473>).

The Accused Instrumentalities receive a subscription message from a first mobile wireless device, the subscription message indicating that the first mobile wireless device is subscribing to a service.

In particular, a user subscribes to the iMessage service (a “service”) by activating iMessage on an iPhone. The activation includes a phone number based authentication method whereby a phone number of an iPhone is verified by a carrier network and subscriber identity module (SIM) corresponding to the iPhone. This process also includes the iPhone generating public keys that are sent to Apple’s servers for storage in the Apple Identity Service (IDS). A message sent by the iPhone and received by Apple’s servers in connection with the phone number based authentication process is a “subscription message indicating that the first mobile wireless device is subscribing to a service.” Alternatively, the encryption keys sent by the iPhone and received by Apple’s servers are part of a “subscription message indicating that the first mobile wireless device is subscribing to a service.”

If you can’t turn on or sign in to iMessage or FaceTime on your iPhone

To use either iMessage or FaceTime, you need to activate them on your iPhone. If you see an error message when you try to activate, follow these steps.

When activating iMessage or FaceTime, you might see one of these messages:

- Waiting for activation
- Activation unsuccessful
- An error occurred during activation
- Could not sign in, please check your network connection
- Unable to contact the iMessage server. Try again.

What you need before you sign in

- Make sure that you’re connected to a [cellular data](#) or [Wi-Fi](#) network.
- Make sure that your device has the [latest version of iOS](#).
- Make sure that [your time zone is set correctly](#). Go to Settings > General > Date & Time.

If you’re using an iPhone, you need SMS messaging to activate your phone number with iMessage and FaceTime. Depending on your carrier, you might be charged for this SMS.

If a prompt appears stating “Your network provider may charge for SMS messages used to activate FaceTime and iMessage”, tap “Turn On” to allow possible SMS charges.

HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

	Exhibit 18, If you can’t turn on or sign in to iMessage, https://support.apple.com/en-us/119859. iMessage security overview ... As users enable additional devices for use with iMessage, their encryption and signing public keys, APNs addresses, and associated phone numbers are added to the directory service. Users can also add more email addresses, which are verified by sending a confirmation link. Phone numbers are verified by the carrier network and SIM. With some networks, this requires using SMS (the user is presented with a confirmation dialog if the SMS isn’t zero rated). Phone number verification may be required for several system services in addition to iMessage, such as FaceTime and iCloud. All of the user’s registered devices display an alert message when a new device, phone number, or email address is added. Exhibit 19, Apple Platform Security – May 2024, at 196. <i>The iMessage service is a service for sending and receiving messages other than Short Message Service (SMS) messages, Enhanced Messaging Service (EMS) messages and Multimedia Messaging Service (MMS) messages.</i> Specifically, Apple’s iMessage service is a packet switched message service for sending and receiving packet-switched messages (e.g., iMessages) which are not SMS, EMS or MMS 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.

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

HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

receives a first request, from the first mobile wireless device via the base station, the first request comprising a numeric identifier in the format of a phone number, wherein the numeric identifier is retrieved, by the first mobile wireless device, from a message being composed;	The Accused Instrumentalities receive a first request, from the first mobile wireless device via the base station, the first request comprising a numeric identifier in the format of a phone number, wherein the numeric identifier is retrieved, by the first mobile wireless device, from a message being composed. <i>The Accused Instrumentalities receive a first request, from the first mobile wireless device via the base station, the first request comprising a numeric identifier in the format of a phone number.</i> In particular, upon initiating a new message in a new conversation, a device of the Accused Instrumentalities retrieves a phone number from a new message and sends it in a request to the IDS. 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. 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. Exhibit 17, Apple Brief, dated 6/15/22, at 6.
---	---

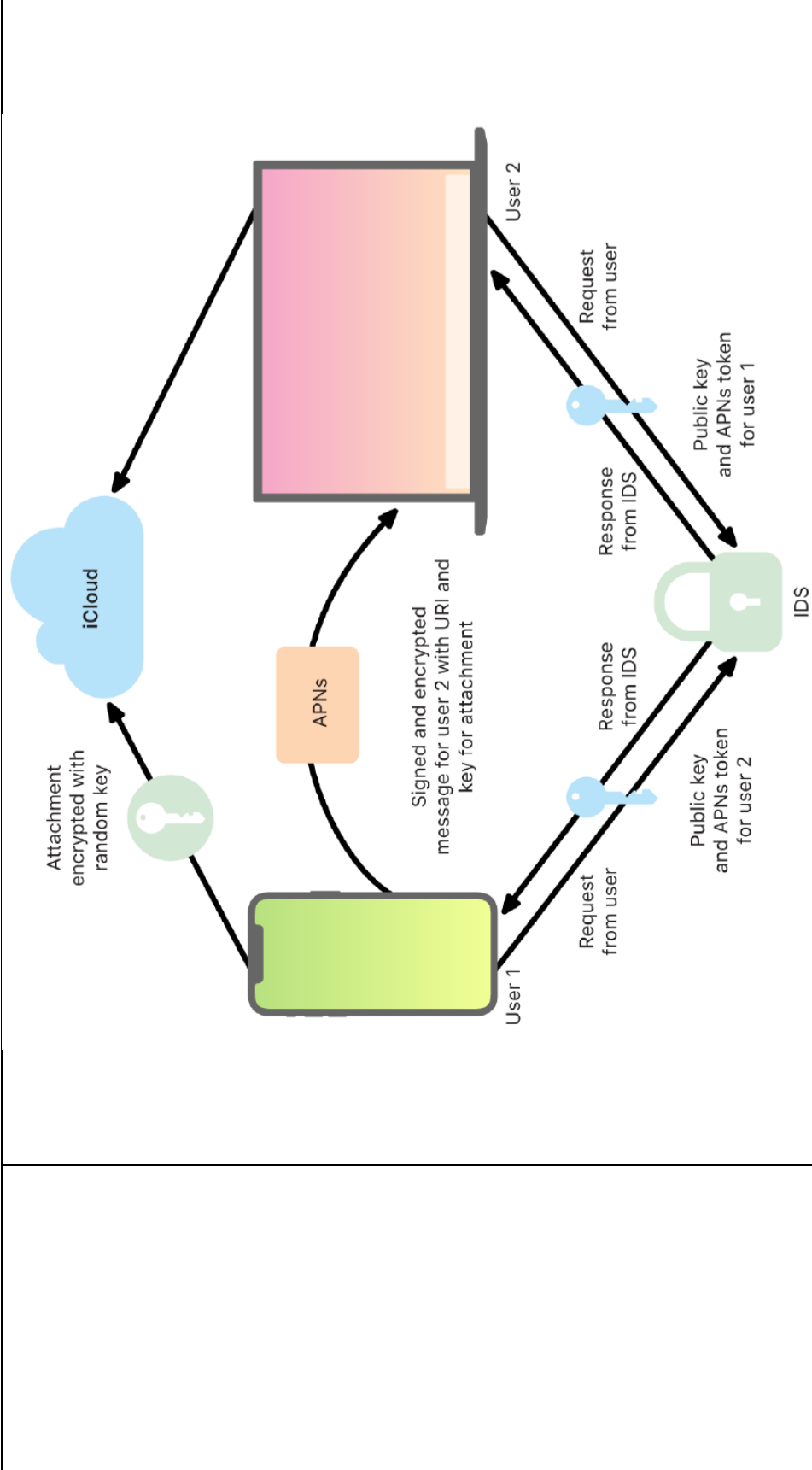


Exhibit 19, Apple Platform Security – May 2024, at 198.

The numeric identifier is retrieved, by the first mobile wireless device, from a message being composed.

The patent specification describes that the message includes the destination phone number. Figure 6B, for example, demonstrates this teaching:

FIG. 6B

```
<message>
<to>
+1 555 1234
</to>
<body>
Hi there!
</body>
<attachment>
<photo>
0xf6,0x34,0xa7...
</photo>
<voicemail>
0xf6,0x34,0xa7...
</voicemail>
</attachment>
</message>
```

See also ‘601 patent at 5:58. The specification describes other examples. See, e.g., *id.* at 7:16-50.

The Accused Instrumentalities operate in the same manner. In particular, the Accused Instrumentalities retrieve a phone number (a “numeric identifier”) from a message being composed.

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.

Exhibit 17, Apple Brief, dated 6/15/22, at 6.

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

HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

retrieve the public keys and APNs addresses for all of the devices associated with the addressee.

Exhibit 19, Apple Platform Security – May 2024, at 197.

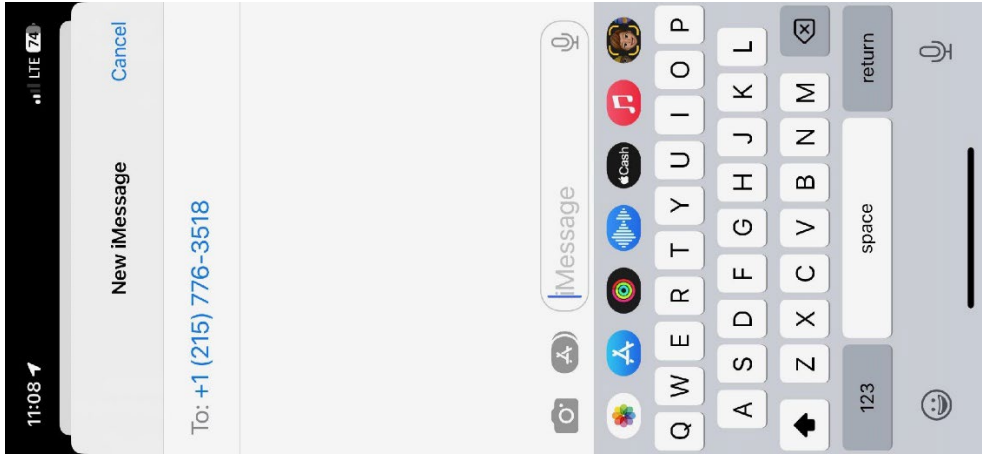


Exhibit 20, Apple iPhone Screenshot taken August 26, 2024.

HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

determines that an email address is associated with the numeric identifier and that the email address is associated with a second mobile wireless device;	The Accused Instrumentalities determine that an email address is associated with the numeric identifier and that the email address is associated with a second mobile wireless device. <i>The Accused Instrumentalities determine that an email address is associated with the numeric identifier and that the email address is associated with a second mobile wireless device.</i> In particular, at least some messages between iMessage subscribers are routed via an email address associated with the phone number of the addressee. For example, in at least some cases when a sending iPhone addresses a message to an iMessage subscriber using the recipient's phone number, and the recipient has both an iPhone and an iPad lacking cellular capability, the message is routed to the iPad (“the second mobile wireless device”) based on an email address that is associated with the recipient's phone number in the IDS. iMessage security overview ... When a user turns on iMessage on a device, the device generates encryption and signing pairs of keys for use with the service. ... The public keys are sent to Apple Identity Service (IDS), where they are associated with the user’s phone number or email address, along with the device’s APNs address. As users enable additional devices for use with iMessage, their encryption and signing public keys, APNs addresses, and associated phone numbers are added to the directory service. Users can also add more email addresses, which are verified by sending a confirmation link. ... Exhibit 19, Apple Platform Security – May 2024, at 196. 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.
---	--

HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

	Exhibit 17, Apple Brief, dated 6/15/22, at 6. 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. Exhibit 19, Apple Platform Security – May 2024, at 197.
sends, based on the determination that the email address is associated with the second mobile wireless device, a first response to the first request, to the first mobile wireless device, the first response indicating that a message to the second mobile wireless device is to be sent via the service;	The Accused Instrumentalities send, based on the determination that the email address is associated with the second mobile wireless device, a first response to the first request, to the first mobile wireless device, the first response indicating that a message to the second mobile wireless device is to be sent via the service. <i>The Accused Instrumentalities send, based on the determination that the email address is associated with the second mobile wireless device, a first response to the first request, to the first mobile wireless device, the first response indicating that a message to the second mobile wireless device is to be sent via the service.</i> As noted above, in at least some cases when a sending iPhone addresses a message to an iMessage subscriber using the recipient's phone number, and the recipient has both an iPhone and an iPad lacking cellular capability, the message is routed to the iPad (“the second mobile wireless device”) based on an email address that is associated with the recipient's phone number in the IDS. Specifically, in response to an iPhone sending a request with a phone number of an intended recipient to the IDS, the IDS determines whether the phone number corresponds to an iMessage subscriber and whether an email address is associated with the phone number of the intended recipient. Such an email address would correspond, e.g., to the email address of the iPad mentioned above (“the second mobile wireless device.”) If there is an associated email address, the IDS provides a response that includes public keys of the addressed recipient, indicating that the message is to be sent via the iMessage service to the second mobile wireless device.

	iMessage security overview ... When a user turns on iMessage on a device, the device generates encryption and signing pairs of keys for use with the service. ... The public keys are sent to Apple Identity Service (IDS), where they are associated with the user’s phone number or email address, along with the device’s APNs address. As users enable additional devices for use with iMessage, their encryption and signing public keys, APNs addresses, and associated phone numbers are added to the directory service. Users can also add more email addresses, which are verified by sending a confirmation link. ... Exhibit 19, Apple Platform Security – May 2024, at 196. 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. Exhibit 17, Apple Brief, dated 6/15/22, at 6. 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. Exhibit 19, Apple Platform Security – May 2024, at 197.
receives a second request, from the first mobile wireless device, the second request	The Accused Instrumentalities receive a second request, from the first mobile wireless device, the second request comprising another phone number which is different than the numeric identifier.

HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

comprising another phone number which is different than the numeric identifier; and	<i>The Accused Instrumentalities receive a second request, from the first mobile wireless device, the second request comprising another phone number which is different than the numeric identifier.</i> In particular, upon initiating a new message in a new conversation with a different recipient, a device of the Accused Instrumentalities retrieves another phone number (which is different from the numeric identifier) from the new message and sends as part of a second request to the IDS. The IDS receives the second request. 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. 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. Exhibit 17, Apple Brief, dated 6/15/22, at 6.
---	--

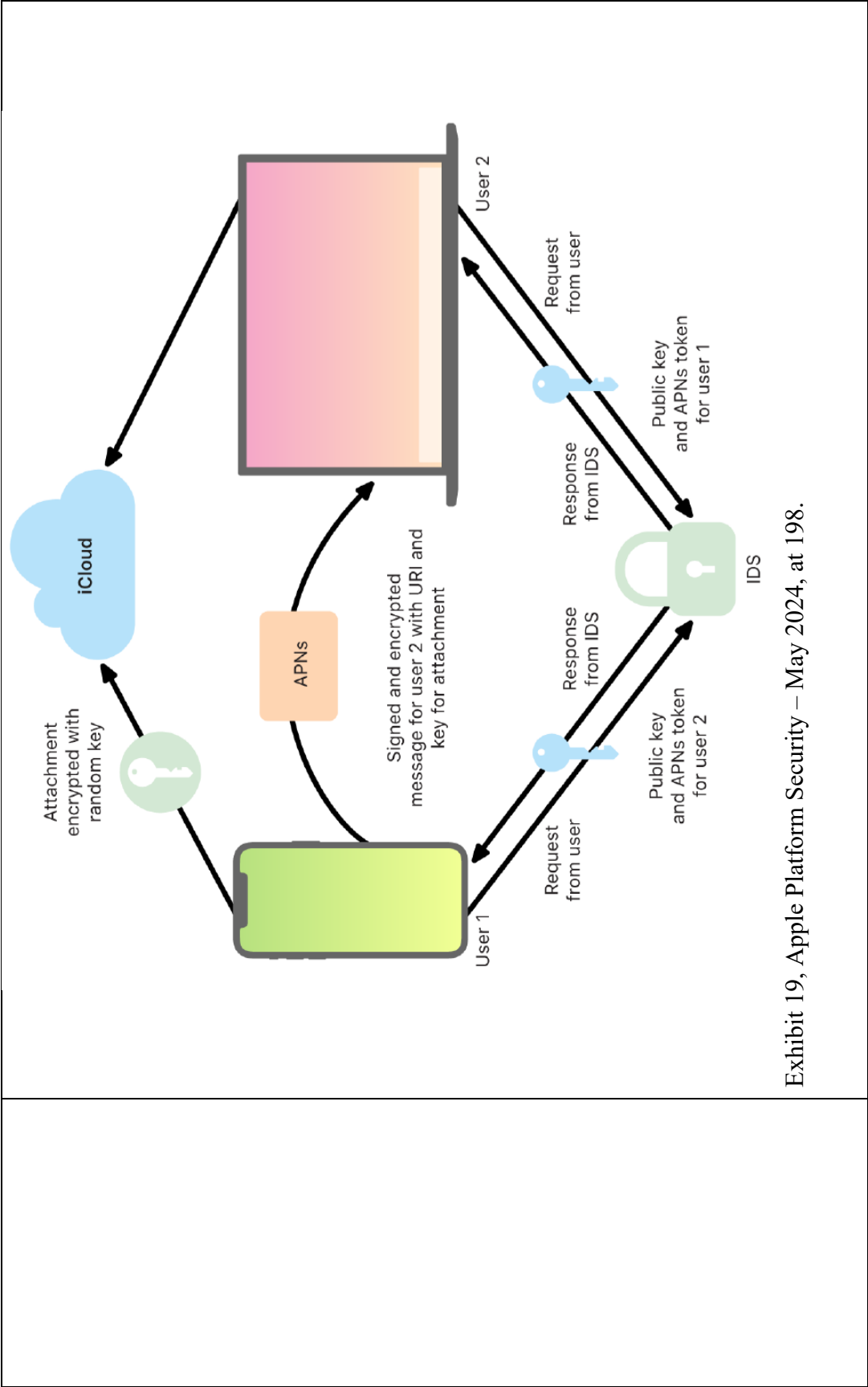


Exhibit 19, Apple Platform Security – May 2024, at 198.

HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

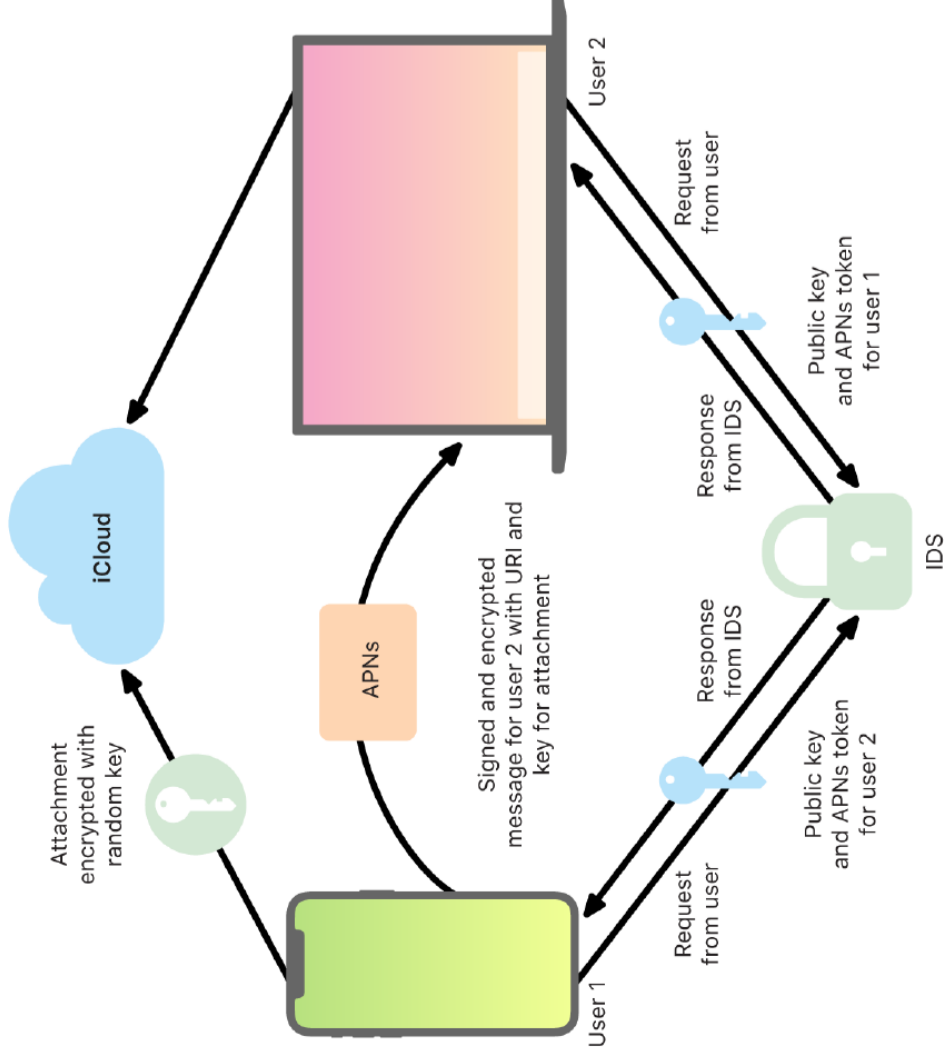
sends a second response to the second request, to the first mobile wireless device, the second response indicating that a message to a third mobile wireless device is not to be sent via the service.	The Accused Instrumentalities send a second response to the second request, where the second response indicates that a message to a third mobile device is not to be sent via the service. <i>The Accused Instrumentalities send a second response to the second request that indicates that a message to a third mobile device is not to be sent via the service.</i> Specifically, at least in a case where the iPhone user is starting a new conversation with a new recipient (associated with “a third mobile wireless device”) that does not correspond to an iMessage subscriber, the IDS send a second response to the second request which lacks encryption keys for the addressed recipient. By failing to return encryption keys, the second response indicates that a message to a third mobile wireless device is to be sent via SMS rather than via the iMessage service. 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 ... Exhibit 17, 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. Exhibit 17, Apple Brief, dated June 15, 2022, at 5-6.
---	---

HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

26. The system of claim 25, wherein the server system determines that the second mobile wireless device is inactive, subsequent to the second response being sent; wherein the server system provides information indicating that messages to the second mobile wireless device should not be sent via the service, to a plurality of mobile wireless devices.	The Accused Instrumentalities include a server system that determines that the second mobile wireless device is inactive, subsequent to the second response being sent. The server system provides information indicating that messages to the second mobile wireless device should not be sent via the service, to a plurality of mobile wireless devices. <i>The server system determines that the second mobile wireless device is inactive, subsequent to the second response being sent.</i> Specifically, encryption keys will be returned by the IDS in response to a request including the phone number of the second mobile wireless device when, e.g., the second mobile wireless device is registered for iMessage and has not missed a heartbeat. In a case where the second mobile phone has gone offline subsequent to the second response being sent and has missed a “heartbeat” (because, e.g., the time for sending the next heartbeat has not been reached), the second receiving mobile phone will given an inactive status. In a case where the IDS receives requests from a plurality of other sending phones which include the phone number of the second mobile wireless device after the second mobile wireless device has transitioned to an inactive status, the IDS will provide responses that lack encryption keys, indicating to the plurality of other sending devices that messages to the second mobile wireless device should be sent via SMS rather than the iMessage service. 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. ... Exhibit 17, Apple Brief, dated June 15, 2022, at 5.
---	--

HBCU MESSAGING US'S FIRST INFRINGEMENT ANALYSIS

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.



HBCU MESSAGING US’S FIRST INFRINGEMENT ANALYSIS

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