

EXHIBIT 4

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

U.S. Patent No. 11,653,182 – Apple Inc.

Claim 17

HBCU Messaging US LP (“HBCU”) provides evidence of infringement of claim 17 of U.S. Patent No. 11,653,182 (hereinafter “the ’182 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 ’182 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 ’182 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 LP’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 '182 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.

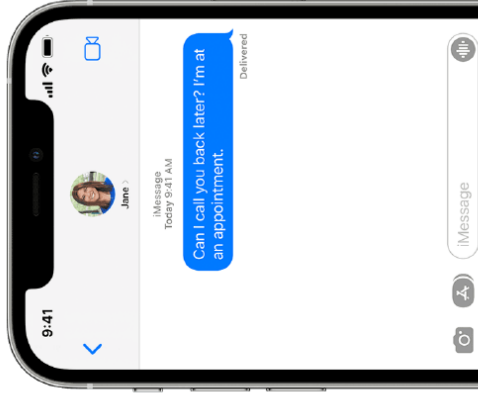
Claim 17	Accused Instrumentalities
<p>17. A method performed by a sending mobile phone that transmits short message service (SMS) messages via a cellular network and packet switched messages via a packet switched message service (PSMS), the method comprising:</p>	<p>The Accused Instrumentalities include 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).</p> <p><i>The Accused Instrumentality includes a sending mobile phone that transmits SMS messages via a cellular network.</i></p> <p>Specifically, the iMessage system on the Apple iPhone sends SMS messages to other cell phones that appear in green bubbles on the iPhone device.</p>

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?

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

[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 16, Apple Brief, dated 6/15/22, at 5.

The Accused Instrumentality 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 to other Apple iPhones that appear in blue bubbles on an iPhone device. These non-SMS messages are packet switched messages sent over Wi-Fi or cellular data networks. The iMessage service is a packet switched message service.

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?

HBCU MESSAGING US LP’S FIRST INFRINGEMENT ANALYSIS

	<p>[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.</p> <p>See: Exhibit 16, Apple Brief, dated 6/15/22, at 5.</p>
<p>authenticating a phone number of the sending mobile phone with the PSMS;</p>	<p>The Accused Instrumentalities authenticate a phone number of the sending mobile phone with the PSMS.</p> <p><i>The Accused Instrumentalities authenticate a phone number of the sending mobile phone with the PSMS.</i></p> <p>In particular, the iPhone uses 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.</p>

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.

See: 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

HBCU MESSAGING US LP’S FIRST INFRINGEMENT ANALYSIS

	<p>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.</p> <p>See: Exhibit 19, Apple Platform Security – May 2024, pg 196</p>
<p>sending first information representing a phone number of a first receiving mobile phone to a server of the PSMS;</p>	<p>The Accused Instrumentalities send first information representing a phone number of a first receiving mobile phone to a server of the PSMS.</p> <p><i>The Accused Instrumentalities send first information representing a phone number of a first receiving mobile phone to a server of the PSMS.</i></p> <p>Specifically, for example, upon initiating a new message in a new conversation, an iOS device retrieves a phone number from the new message and sends it to the Apple Identity Services (“IDS”). The IDS is a server of the PSMS.</p>

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

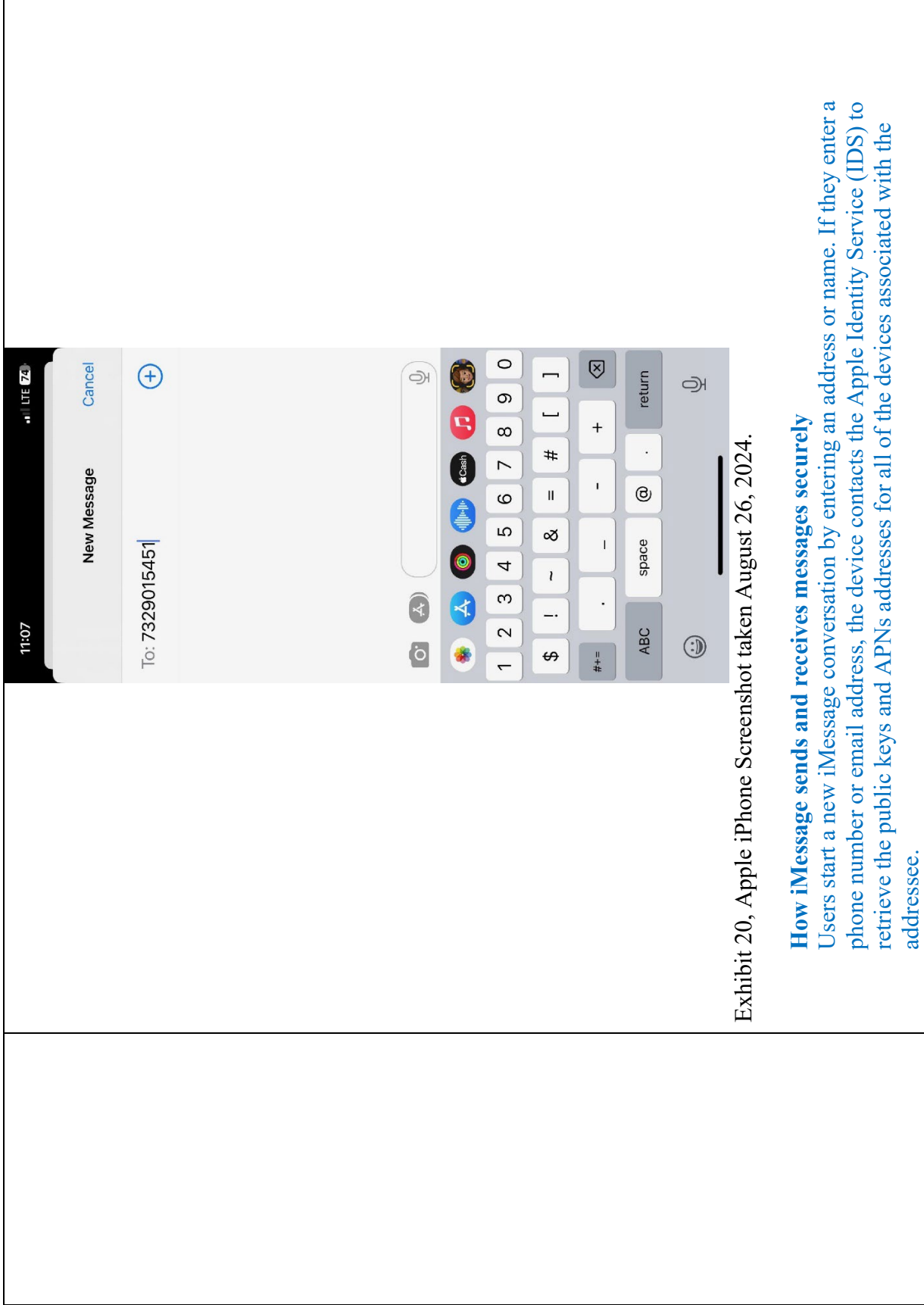


Exhibit 20, Apple iPhone Screenshot taken August 26, 2024.

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 address.

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

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

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. For encryption, there is an encryption RSA 1280-bit key as well as an encryption EC 256-bit key on the NIST P-256 curve. For signatures, Elliptic Curve Digital Signature Algorithm (ECDSA) 256-bit signing keys are used. The private keys are saved in the device's keychain and only available after first unlock. 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.

...

See: Exhibit 19, Apple Platform Security – May 2024, pg 196

The Accused Instrumentalities send the first receiving mobile phone number to a server.

Specifically, the sending mobile phone sends a request message that includes the first receiving mobile phone number to the Apple Identity Service (IDS) database. While, in the below diagram from the Apple Security Guide, 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.

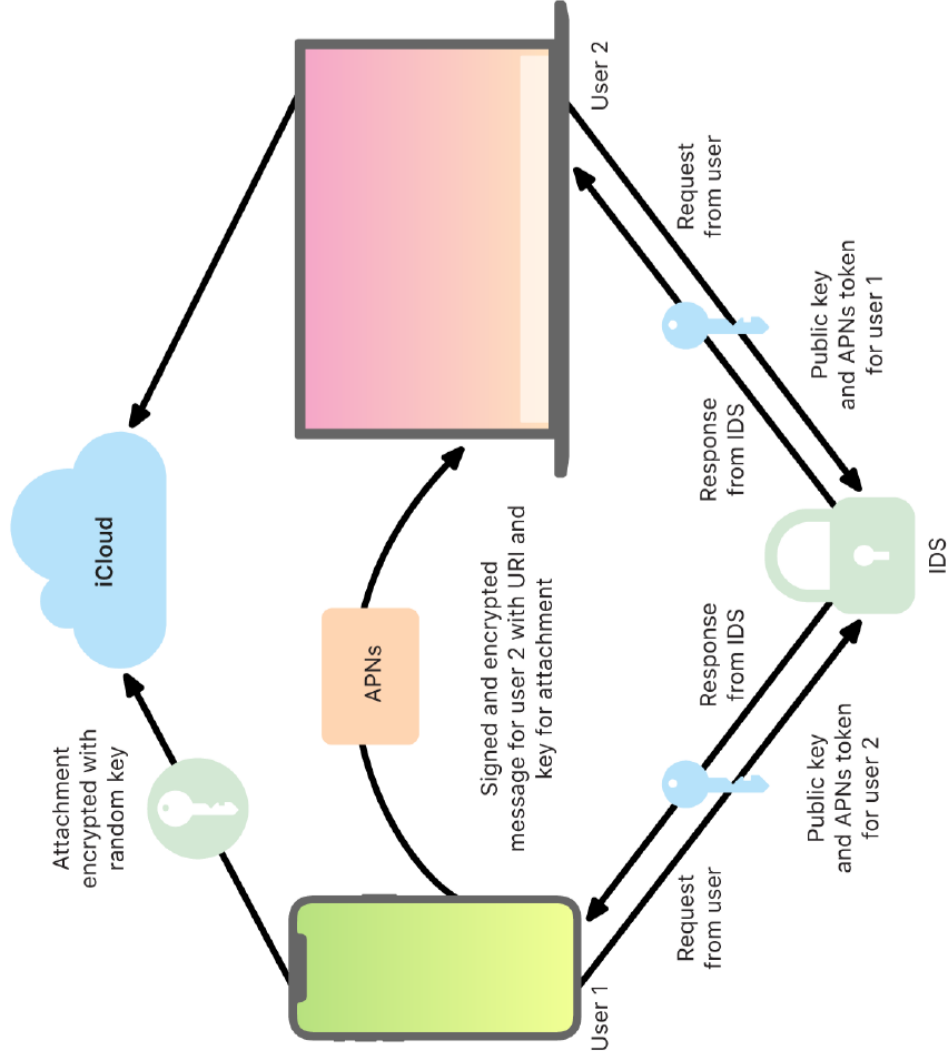
See: Exhibit 19, Apple Platform Security – May 2024, at 197.

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

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.

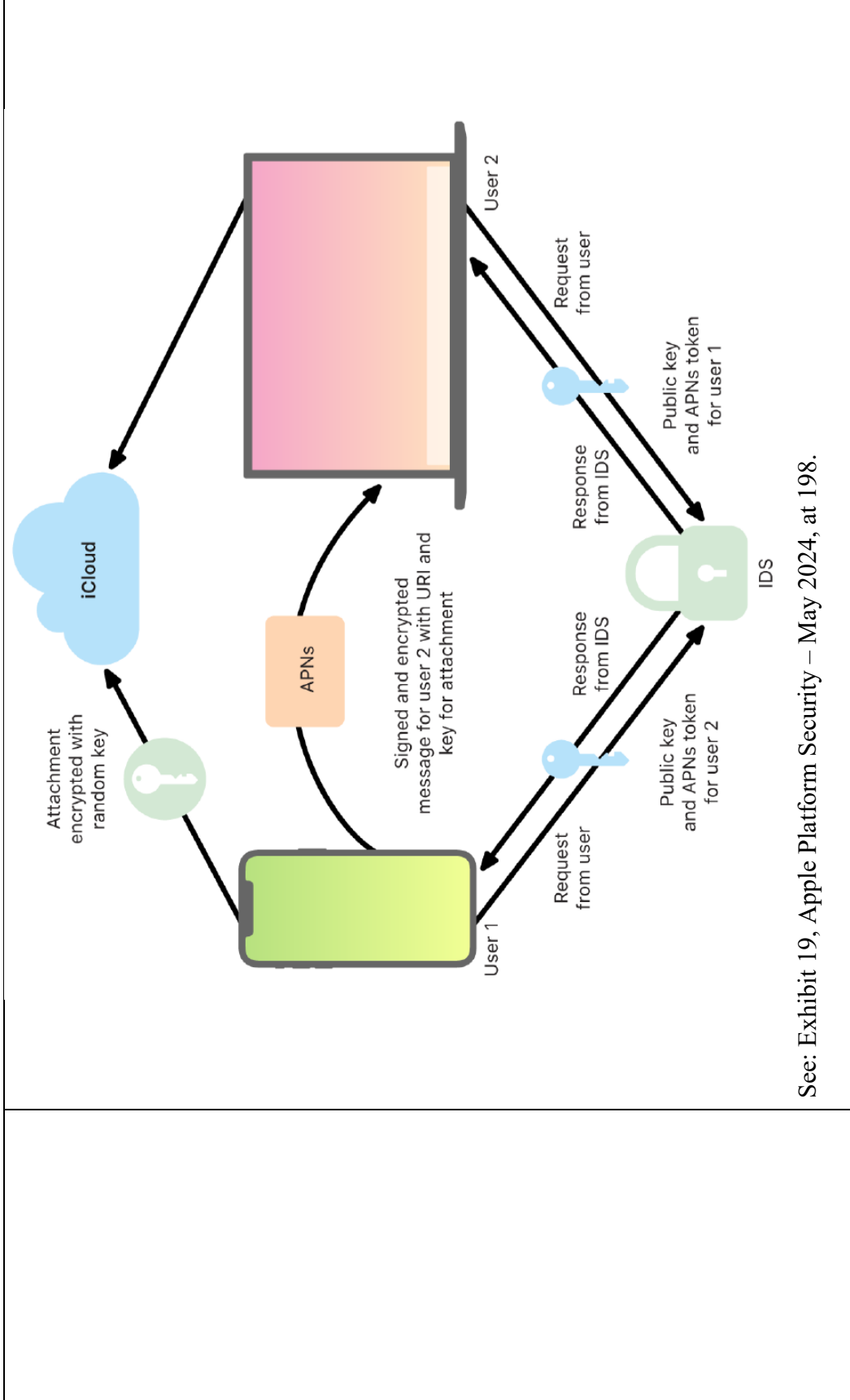
See: Exhibit 17, Apple Brief, dated 6/15/22, at 6.



HBCU MESSAGING US LP’S FIRST INFRINGEMENT ANALYSIS

<p>receiving a first response when the phone number of the first receiving mobile phone is not identified as a subscriber of the PSMS;</p>	<p>See: Exhibit 19, Apple Platform Security – May 2024, at 198.</p> <p>The Accused Instrumentalities receive a first response when the phone number of the first receiving mobile phone is not identified as a subscriber of the PSMS.</p> <p><i>The Accused Instrumentalities receive a first response when the phone number of the first receiving mobile phone is not identified as a subscriber of the PSMS.</i></p> <p>In particular, in response to the sending mobile phone sending a request message the IDS sends a response to the sending mobile phone. When the IDS does not identify a phone number as a subscriber, the response does not include public keys of an addressed recipient.</p> <p>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.</p> <p>...</p> <ol style="list-style-type: none">1. Request for public keys at the IDS database <p>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.</p> <ol style="list-style-type: none">a) Public keys are stored in the IDS database if<ul style="list-style-type: none">• the receiving device is registered for iMessage and ... <p>See: Exhibit 17, Apple Brief, dated June 15, 2022, at 5, 6</p>
--	---

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS



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

sending, after the first response is received by the sending mobile phone, an SMS message

The Accused Instrumentalities send, after the first response is received by the sending mobile phone, an SMS message to the first receiving mobile phone.

After the first response is received by the sending mobile phone, an SMS message is sent to the first receiving mobile phone.

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

to the first receiving mobile phone;

In particular, when the sending iPhone fails to receive keys in the response, the sending iPhone transmits the message via SMS.

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.

...

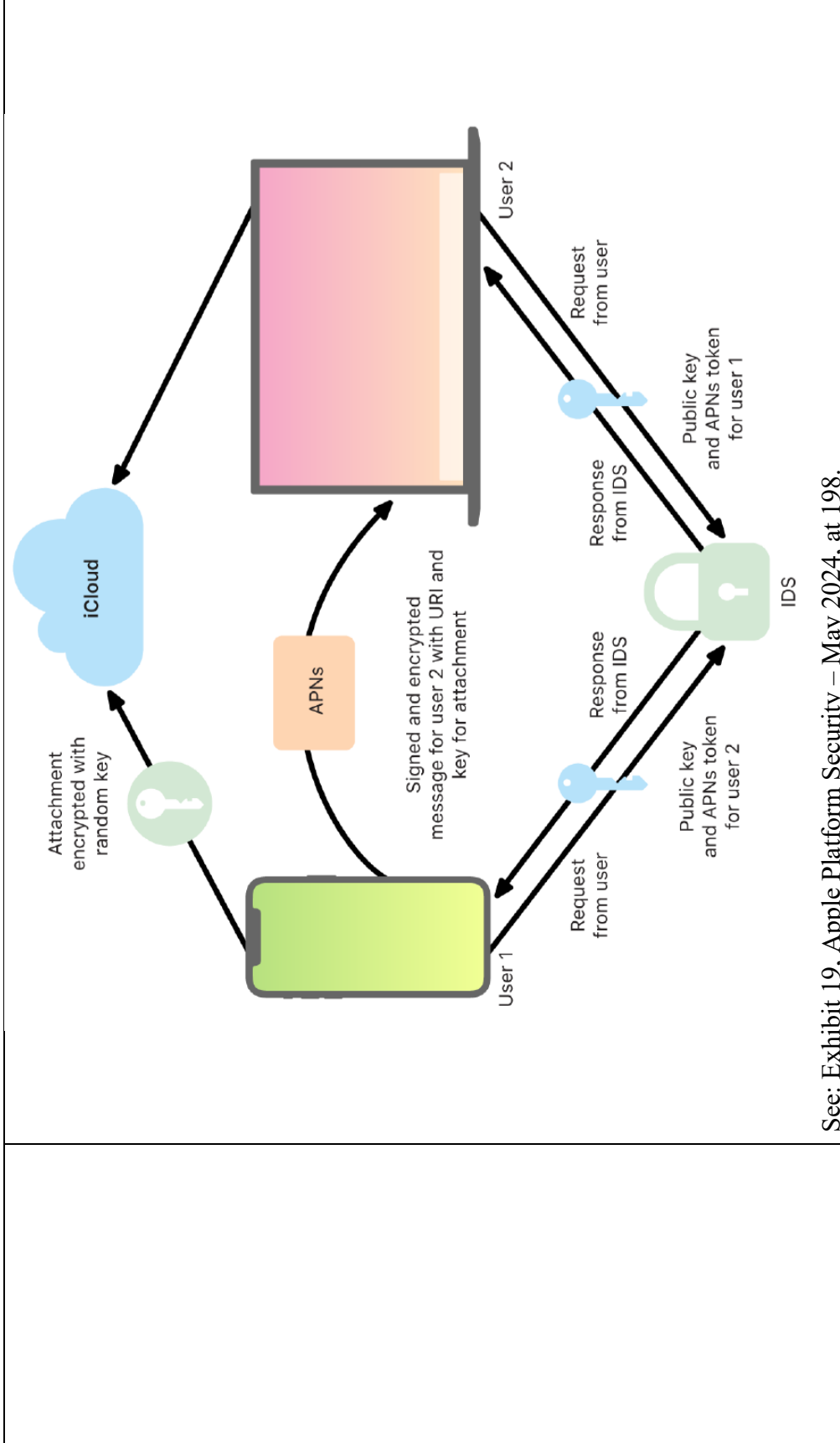
1. Request for public keys at the IDS database

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

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS



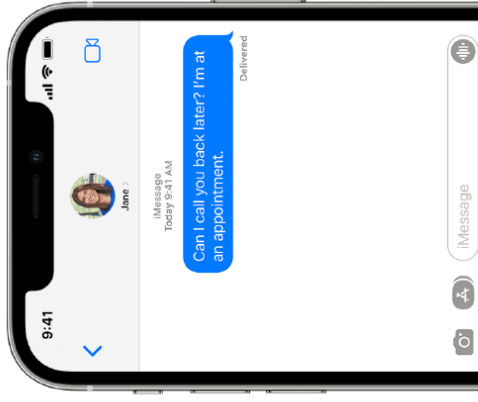
See: Exhibit 19, Apple Platform Security – May 2024, at 198.

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?

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

<p>sending second information representing a phone number of a second receiving mobile phone to the server;</p>	<p>The Accused Instrumentalities send second information representing a phone number of a second receiving mobile phone to the server.</p> <p><i>Second information representing a phone number of a second receiving mobile phone is sent to the server.</i></p> <p>Specifically, when composing a new message for a new conversation, the user of a sending mobile phone can enter a phone number into the address field of the message</p>
---	--

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

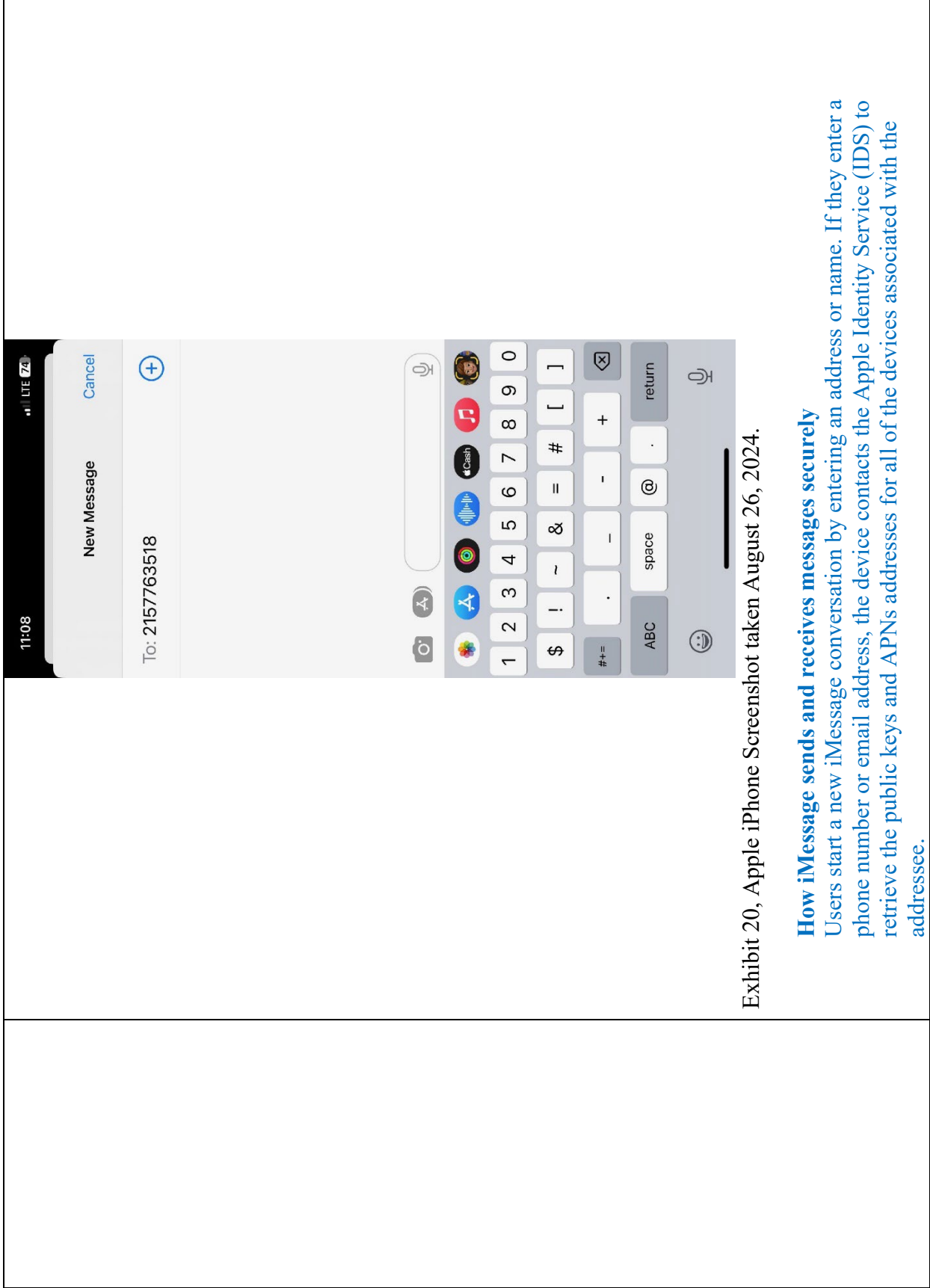


Exhibit 20, Apple iPhone Screenshot taken August 26, 2024.

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.

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

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

The second information is sent to the server.

Upon initiating a new iMessage, an iPhone retrieves a phone number from a new message and sends it 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.

iMessage security overview ...

...

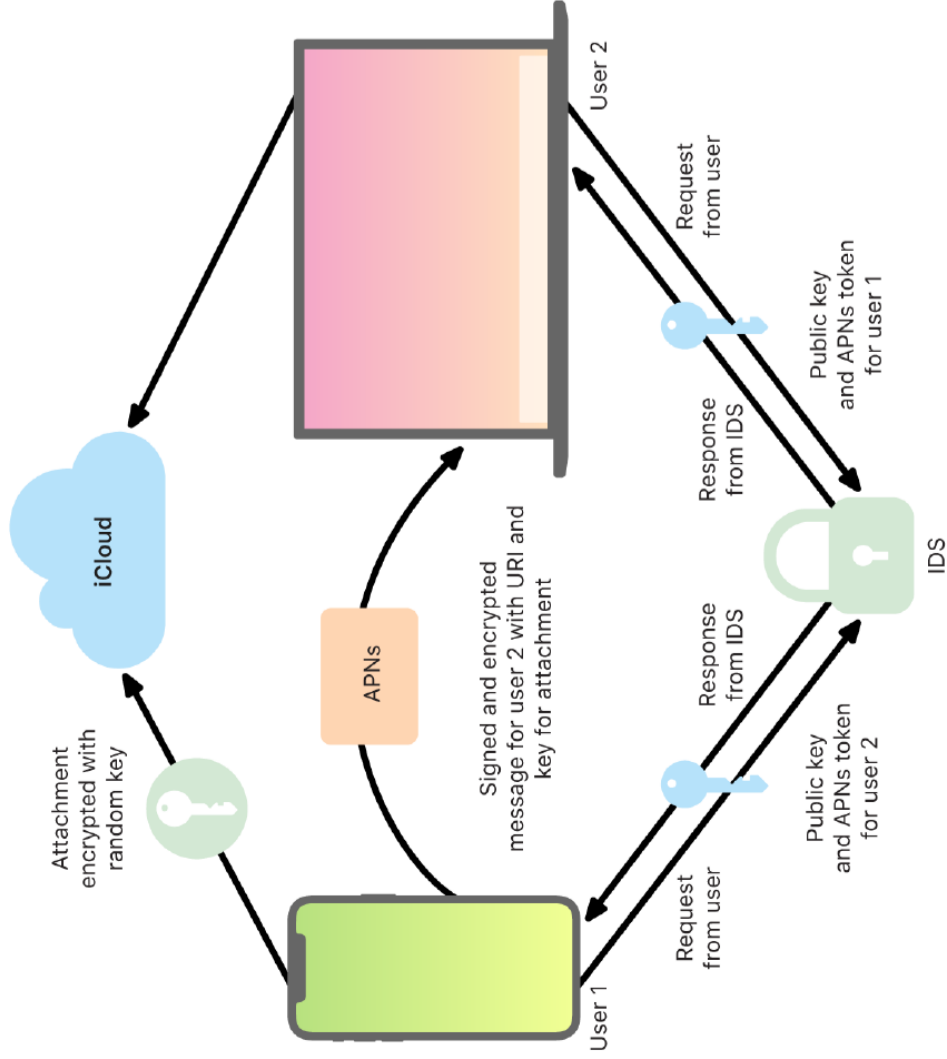
When a user turns on iMessage on a device, the device generates encryption and signing pairs of keys for use with the service. For encryption, there is an encryption RSA 1280-bit key as well as an encryption EC 256-bit key on the NIST P-256 curve. For signatures, Elliptic Curve Digital Signature Algorithm (ECDSA) 256-bit signing keys are used. The private keys are saved in the device's keychain and only available after first unlock. The public keys are sent to Apple Identity Service (IDS), where they are associated

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

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.

...

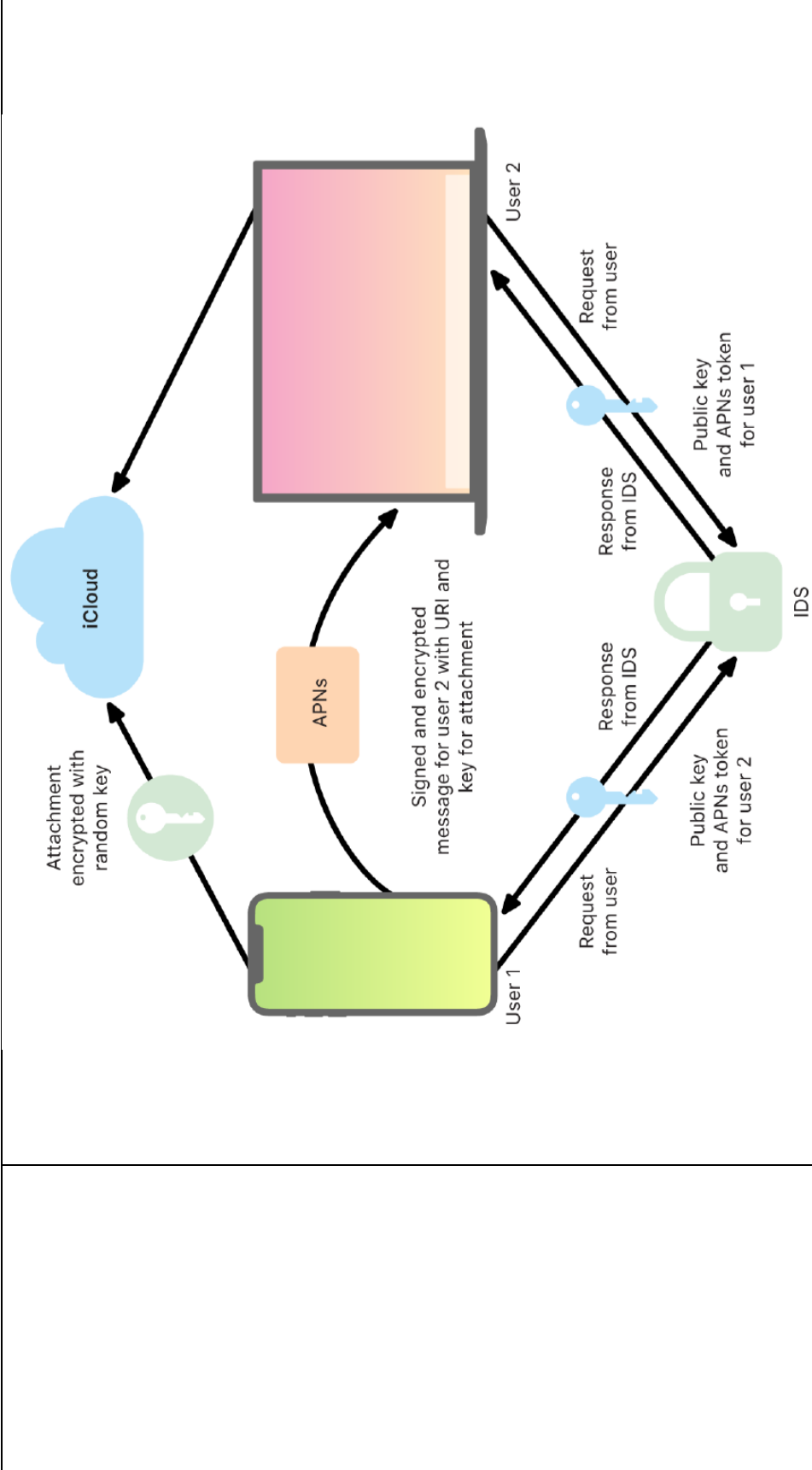
See: Exhibit 19, Apple Platform Security – May 2024, pg 196



HBCU MESSAGING US LP’S FIRST INFRINGEMENT ANALYSIS

<p>receiving a second response, when the phone number of the second receiving mobile phone is identified as a subscriber of the PSMS and when the second receiving mobile phone has an active status with the PSMS; and</p>	<p>See: Exhibit 19, Apple Platform Security – May 2024, at 198.</p> <p>The Accused Instrumentalities receive a second response, when the phone number of the second receiving mobile phone is identified as a subscriber of the PSMS and when the second receiving mobile phone has an active status with the PSMS.</p> <p><i>A second response is received.</i></p> <p>In particular, an iPhone receives a response to the request. The IDS indicates that a subscriber is associated with the PSMS and provides public keys of an addressed recipient.</p> <p>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.</p> <p>...</p> <p>1. Request for public keys at the IDS database</p> <p>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.</p> <p>a) Public keys are stored in the IDS database if</p> <ul style="list-style-type: none"> ● the receiving device is registered for iMessage and ... <p>See: Exhibit 17, Apple Brief, dated June 15, 2022, at 5, 6</p>
---	--

HBCU MESSAGING US LP’S FIRST INFRINGEMENT ANALYSIS



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

The second response is received when the second receiving mobile phone has an active status with the PSMS.

In particular, the IDS maintains status information by tracking “heartbeats” from each iMessage user. If no heartbeats are missed, the subscriber is considered active, so the IDS returns keys in response to an

HBCU MESSAGING US LP’S FIRST INFRINGEMENT ANALYSIS

	<p>address query. When keys are returned in response to the query, it maps to the “second response to the sending mobile phone.”</p> <ol style="list-style-type: none"> 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 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. The intervals at which registered devices must send heartbeats vary from an initial 5 minutes to several weeks. <p>See: Exhibit 17, Apple Brief dated 6/15/22, at 6.</p>
<p>sending a message, after the second response is received by the sending mobile phone, via a wireless local area network (WLAN) and the PSMS, to the second receiving mobile phone;</p>	<p>The Accused Instrumentalities send a message, after the second response is received by the sending mobile phone, via a wireless local area network (WLAN) and the PSMS, to the second receiving mobile phone;</p> <p><i>The Accused Instrumentalities send a message, after the second response is received by the sending mobile phone, via a wireless local area network (WLAN) and the PSMS, to the second receiving mobile phone.</i></p> <p>In particular, an iMessage is sent via a Wi-Fi wireless local area network (WLAN) via APNs.</p>

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.

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: Exhibit 21, Wi-Fi specifications for Apple devices - Apple Support

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.

Published Date: May 29, 2024

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

HBCU MESSAGING US LP’S FIRST INFRINGEMENT ANALYSIS

wherein the second response communicates different information than the first response;

The second response communicates different information than the first response.

In particular, the second response communicates that the second receiving mobile phone corresponds to a subscriber with an active status, while the first response communicates that such conditions are not met for the first receiving mobile phone.

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

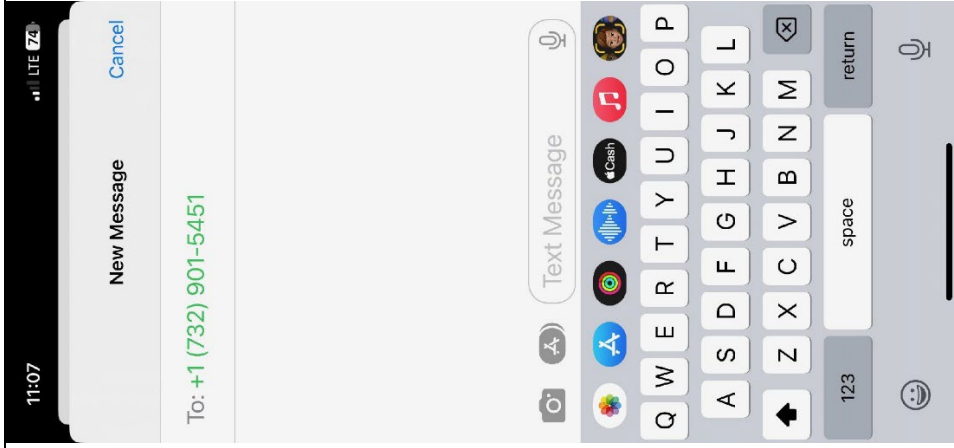


Exhibit 20, Apple iPhone Screenshot taken August 26, 2024.

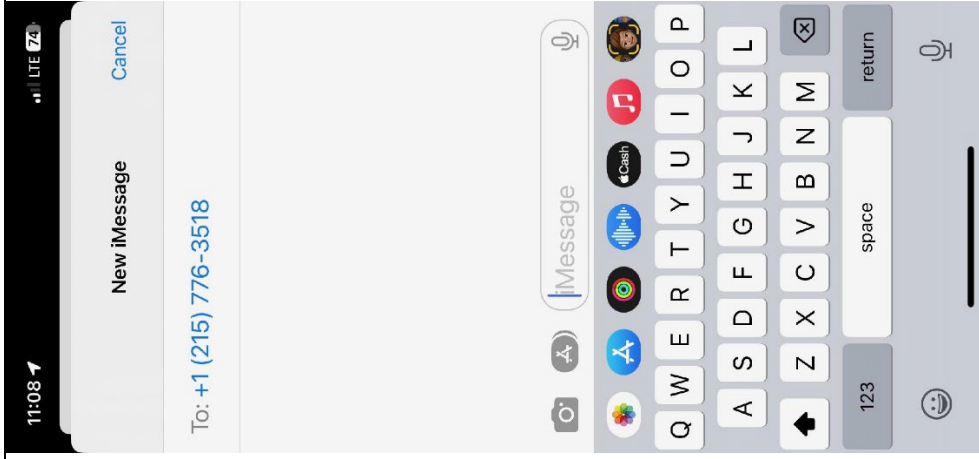


Exhibit 20, Apple iPhone Screenshot taken August 26, 2024.

1. Request for public keys at the IDS database

HBCU MESSAGING US LP’S FIRST INFRINGEMENT ANALYSIS

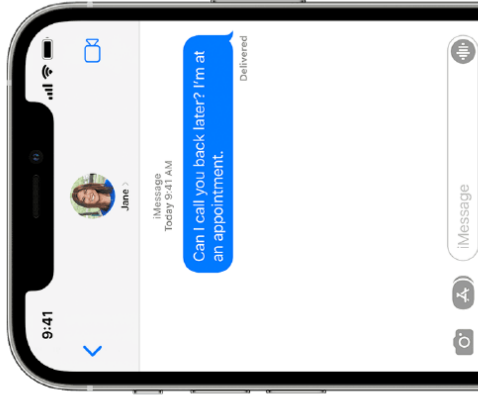
	<p>When composing a message, the sending device checks whether public keys are available for the receiving device in the IDS database...</p> <p>a) Public keys are stored in the IDS database if ...</p> <p>the receiving device sends system messages (so-called heartbeats) to the IDS database. These heartbeats must be sent to the IDS database by each device registered with iMessage at increasing intervals. The intervals at which registered devices must send heartbeats vary from an initial 5 minutes to several weeks.</p> <p>See: Exhibit 17, Apple Brief, dated 6/15/22, at 6.</p>
<p>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;</p>	<p>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.</p> <p><i>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.</i></p> <p>Specifically, Apple's iMessage service is a packet switched message service that does not use SMS, EMS or MMS for sending messages.</p> <p>[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.</p> <p>See: Exhibit 17, Apple Brief, dated 6/15/22, at 5.</p>

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?

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

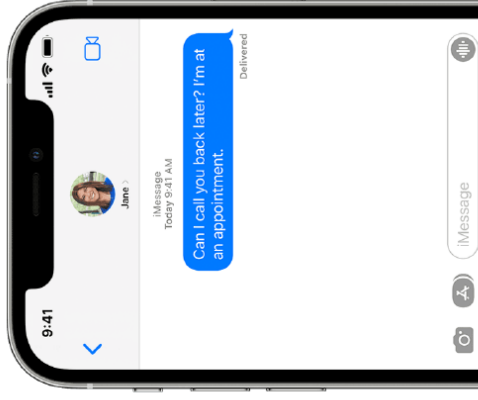
<p>wherein the SMS message sent to the first receiving mobile phone and the message sent to the second receiving mobile phone are originated via a same messaging client.</p>	<p>The SMS message sent to the first receiving mobile phone and the message sent to the second receiving mobile phone are originated via a same messaging client.</p> <p><i>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.</i></p> <p>Specifically, the iPhone includes a common messaging client that displays SMS messages and iMessages. The same messaging client corresponds to the Apple "Messages App".</p>
---	---

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?

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

20. The method of claim 17, wherein when the second response is received, the second receiving mobile phone is offline from the PSMS, wherein the PSMS routes at least some messages between PSMS subscribers according to an email address.

When the second response is received, the second receiving mobile phone is offline from the PSMS, wherein the PSMS routes at least some messages between PSMS subscribers according to an email address.

When the second response is received, the second receiving mobile phone is offline from the PSMS.

In particular, the IDS maintains subscription heartbeat information current to 5 minute intervals. The IDS responds to the request with public keys of a recipient even in scenarios in which a receiving mobile wireless device is not connected to the 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

...

- in addition, 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. The intervals at which registered devices must send heartbeats vary from an initial 5 minutes to several weeks.

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

How iMessage sends and receives messages securely

On the receiving side, each device receives its copy of the message from APNs and, if necessary, retrieves the attachment from iCloud. The incoming phone number or email address of the sender is matched to the receiver's contacts so that a name can be displayed when possible.

As with all push notifications, the message is deleted from APNs when it's delivered. Unlike other APNs notifications, however, iMessage messages are queued for delivery to offline devices. Messages are stored on Apple servers for up to 30 days.

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

The PSMS routes at least some messages between PSMS subscribers according to an email address.

In particular, at least some messages between iMessage subscribers are routed via an email address associated with an addressee. For example: In at least some cases when a sending iPhone sends an iMessage to a subscriber that has both an iPhone and an iPad lacking cellular capability, the message is routed to the iPad based on the Apple ID of the receiving subscriber, where the Apple ID corresponds to an email address ending in ".icloud.com"

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.

See: Exhibit 19, Apple Platform Security – May 2024, pg 196

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.

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

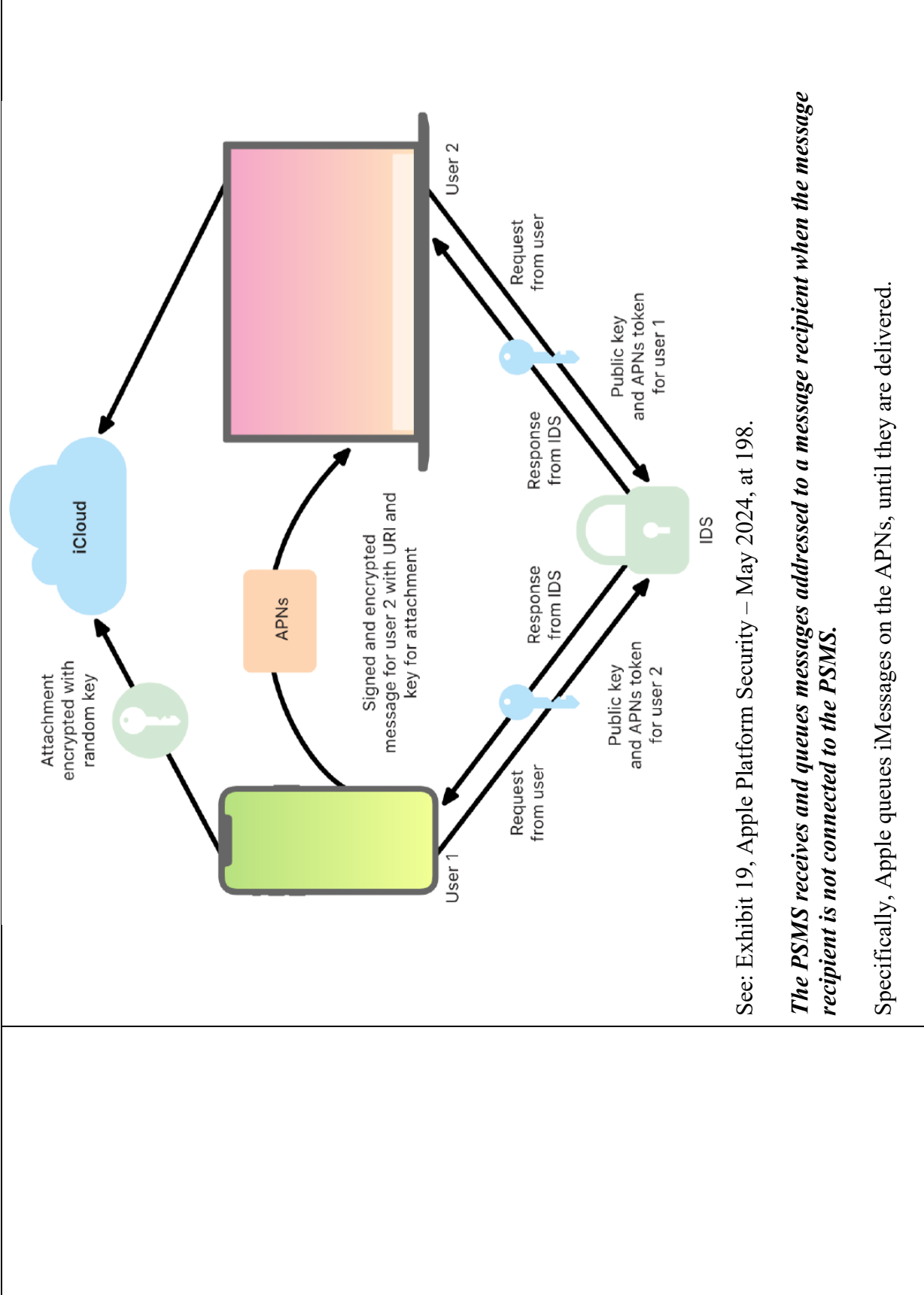
21. The method of claim 17, wherein the server is located outside of the cellular network, wherein the PSMS receives and queues messages addressed to a message recipient when the message recipient is not connected to the PSMS.

The server of the Accused Instrumentalities is located outside of the cellular network, wherein the PSMS receives and queues messages addressed to a message recipient when the message recipient is not connected to the PSMS.

The server is located outside of the cellular network.

The Apple IDS is located outside of the cellular network. In the diagram below, both a cell phone (presumably having cellular network access) and a laptop computer are shown as being able to provide requests and receive responses from the IDS.

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS



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

The PSMS receives and queues messages addressed to a message recipient when the message recipient is not connected to the PSMS.

Specifically, Apple queues iMessages on the APNs, until they are delivered.

HBCU MESSAGING US LP'S FIRST INFRINGEMENT ANALYSIS

How iMessage sends and receives messages securely

On the receiving side, each device receives its copy of the message from APNs and, if necessary, retrieves the attachment from iCloud. The incoming phone number or email address of the sender is matched to the receiver's contacts so that a name can be displayed when possible.

As with all push notifications, the message is deleted from APNs when it's delivered. Unlike other APNs notifications, however, iMessage messages are queued for delivery to offline devices. Messages are stored on Apple servers for up to 30 days.

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