Legal Process Guidelines

Government & Law Enforcement outside the United States

These guidelines are provided for use by government and law enforcement agencies outside of the United States when seeking information from Apple's relevant entities providing service in the relevant region or country about users of Apple's devices, products and services. Apple will update these Guidelines as necessary.

In these Guidelines, Apple shall mean the relevant entity responsible for customer/user information in a particular region or country. Apple, as a global company, has a number of legal entities in different jurisdictions which are responsible for the personal information which they collect and which is processed on their behalf by Apple Inc. For example, point of sale information in Apple's Retail entities outside the United States is controlled by Apple's individual Retail entities in each country. Apple Online Store and iTunes related personal information may also be controlled by legal entities outside the United States as reflected in the terms of each service within a specific jurisdiction. Typically Apple's legal entities outside the United States in Australia, Canada, Ireland and Japan are responsible for user data related to Apple services within their regions of responsibility.

All other requests for information regarding Apple customers/users, including customer/user questions about information disclosure, should be directed to https://www.apple.com/privacy/contact/. These Guidelines do not apply to United States government and law enforcement requests made to Apple Inc.

For government and law enforcement information requests, Apple complies with the laws pertaining to global entities that control our data and we provide details as legally required. All requests from government and law enforcement agencies outside of the United States for content stored in our data centers in the United States, with the exception of emergency circumstances (defined below in Emergency Requests), must comply with the United States Electronic Communications Privacy Act (ECPA). A request under a Mutual Legal Assistance Treaty or Agreement with the United States is in compliance with ECPA.

For private party requests Apple complies with the laws pertaining to local entities that control user data and provides data as legally required.

Apple has a centralized process for receiving, tracking, processing, and responding to legitimate legal requests from government, law enforcement, and private parties from when they are received until when a response is provided. A trained team in our legal department reviews and evaluates all requests received, and requests which Apple determines to have no valid legal basis or considers to be unclear, inappropriate or over-broad are challenged or rejected.

INDEX

I. General Information

Apple designs, manufactures, and markets mobile communication and media devices, personal computers, portable digital music players, and sells a variety of related software, services, peripherals, networking solutions, and third-party digital content and applications. Apple's products and services include Mac, iPhone, iPad, iPod, Apple TV, Apple Watch, a portfolio of consumer and professional software applications, the iOS and Mac OS X operating systems, iCloud, and a variety of accessory, service and support offerings. Apple also sells and delivers digital content and applications through the iTunes Store, App Store, iBookstore, and Mac App Store. User information is held by Apple in accordance with Apple's privacy policy and the applicable terms of service/terms and conditions for the particular service offering. Apple is committed to maintaining the privacy of the users of Apple products and services ("Apple users"). Accordingly, information about Apple users will not be released without valid legal process.

The information contained within these Guidelines is devised to provide information to government and law enforcement agencies outside of the United States regarding the legal process that Apple requires in order to disclose electronic information to government and law enforcement outside the United States. These Guidelines are not intended to provide legal advice. The frequently asked questions ("FAQ") section of these Guidelines is intended to provide answers to some of the more common questions that Apple receives. Neither these Guidelines nor the FAQ will cover every conceivable circumstance that may arise.

If you have further questions, please contact the relevant email address for your region, as follows:

Americas (Outside of United States)
Government and law enforcement agencies in the Americas outside the United States (i.e. Canada, Latin America & the Caribbean) should transmit requests from an official government or law enforcement email address to the mailbox: lawenforcement@apple.com.

APAC (Asia Pacific)
Government and law enforcement agencies in the Asia Pacific region should transmit requests from an official government or law enforcement email address to the mailbox: apac_police_requests@apple.com.

EMEIA (Europe, Middle-East, India, Africa)
Government and law enforcement agencies in Europe, the Middle-East, India and Africa should transmit requests from an official government or law enforcement email address to the mailbox: law.enf.emeia@apple.com.

The above email addresses are intended solely for use by government and law enforcement personnel in their respective regions. If you choose to send an email to one of these addresses, it must be from a valid and official government or law enforcement email address.

The majority of law enforcement requests that Apple receives seek information regarding a particular Apple device or customer and the specific service(s) that Apple may provide to that customer. Apple can provide Apple device or customer information in so far as Apple still possesses the requested information pursuant to its data retention policies. Apple retains data as outlined in certain "Information Available" sections below. All other data is retained for the period necessary to fulfill the purposes outlined in our privacy policy. Government and law enforcement agencies should be as narrow and

specific as possible when fashioning their requests to avoid misinterpretation, challenge and/or rejection in response to an unclear, inappropriate, or over-broad request. All requests from government and law enforcement agencies outside of the United States for content stored in our data centers in the United States, with the exception of emergency circumstances (defined below in Emergency Requests), must comply with the United States Electronic Communications Privacy Act (ECPA). A request under a Mutual Legal Assistance Treaty or Agreement with the United States is in compliance with ECPA.

Nothing within these Guidelines is meant to create any enforceable rights against Apple and Apple's policies may be updated or changed in the future without further notice to government or law enforcement.

II. Legal Requests to Apple

A. Government and Law Enforcement Information Requests

Apple accepts service of legally valid government or law enforcement information requests by email from government and law enforcement agencies, provided these are transmitted from the official email address of the government or law enforcement agency concerned. Government and law enforcement personnel outside of the United States transmitting an information request to Apple should complete a Government & Law Enforcement Information Request template and transmit it directly from their official government or law enforcement email address to the relevant email address for their region, as follows:

Americas (Outside of United States)
Government and law enforcement agencies in the Americas outside the United States (i.e. Canada, Latin America & the Caribbean) should transmit requests from an official government or law enforcement email address to the mailbox: lawenforcement@apple.com.

APAC (Asia Pacific)
Government and law enforcement agencies in the Asia Pacific region should transmit requests from an official government or law enforcement email address to the mailbox: apac_police_requests@apple.com.

EMEIA (Europe, Middle-East, India, Africa)
Government and law enforcement agencies in Europe, the Middle-East, India and Africa should transmit requests from an official government or law enforcement email address to the mailbox: law.enf.emeia@apple.com.

The above email addresses are intended solely for use by government and law enforcement personnel in the regions as outlined. If you choose to send an email to one of these addresses, it must be from a valid and official government or law enforcement email address. Where requests contain five or more identifiers, such as Device Serial/IMEI numbers, Apple ID's, Email addresses, or Invoice/ Order numbers, these should be transmitted in an editable format. Identifiers such as these are generally required in order to conduct searches for information related to devices, accounts, or financial transactions.

Apple considers a law enforcement information request to be legally valid if it is made in circumstances where it has a precise legal basis in the domestic law of the requesting country and is pertaining to the bona-fide prevention, detection or investigation of offences. Examples of requests Apple considers to be legally valid and receives internationally are: Production Orders (Australia, Canada), Tribunal Orders (New Zealand), Requisition or Judicial Rogatory Letters (France), Solicitud Datos (Spain), Ordem Judicial (Brazil), Auskunftsersuchen (Germany), 個人情報の開示依頼 (Japan), Personal Data Request (U.K.), as well as equivalent court orders and/or requests from other countries.

B. Managing and Responding to Government and Law Enforcement Requests

Apple carefully reviews all requests from government, law enforcement, and private parties to ensure that there's a valid legal basis for each request; and complies with legally valid requests. In instances where Apple determines that there is no valid legal basis or where a request is considered to be unclear, inappropriate or over-broad Apple will challenge or reject the request.

C. Preservation Requests

All requests from government and law enforcement agencies outside of the United States for content stored in our data centers in the United States, with the exception of emergency circumstances (defined below in Emergency Requests), must comply with the United States Electronic Communications Privacy Act (ECPA). A request under a Mutual Legal Assistance Treaty or Agreement with the United States is in compliance with ECPA. A request to preserve data in advance of impending ECPA compliant request should be sent to Apple Inc. by email to the mailbox: subpoenas@apple.com.

Preservation requests must include the relevant Apple ID/account email address, or full name **and** phone number, and/or full name **and** physical address of the subject Apple account. When a preservation request has been received, Apple Inc. will preserve a one-time data pull of the requested existing user data available at the time of the request for 90 days. After this 90 day period, the preservation will be automatically removed from the storage server. However, this period can be extended one additional 90-day period upon a renewed request. More than two preservations for the same account will be treated as requests for an extension of the originally preserved materials, but Apple Inc. will not preserve new material in response to such requests.

D. Emergency Requests

Apple considers a request to be an emergency request when it relates to circumstance(s) involving imminent and serious threat(s) to:

1) the life/safety of individual(s);
2) the security of a State;
3) the security of critical infrastructure/installation(s).

If the requesting government or law enforcement officer provides satisfactory confirmation that their request relates to emergency circumstance(s) involving one or more of the above criteria, Apple will examine such a request on an emergency basis.

In order to make an emergency request to Apple, the requesting government or law enforcement officer should complete the Emergency Government & Law Enforcement Information Request form and transmit it directly from their official government or law enforcement email address to the mailbox: exigent@apple.com with the words “Emergency Request” in the subject line.

In the event that Apple produces customer data in response to an Emergency Government & Law Enforcement Information Request, a named supervisor for the government or law enforcement agent who submitted the Emergency Government & Law Enforcement Information Request may be contacted and asked to confirm to Apple that the emergency request was legitimate. The government or law enforcement agent who submits the Emergency Government & Law Enforcement Information Request should provide the supervisor's contact information in the request.

If government or law enforcement needs to contact Apple after hours (before 8:00 am or after 5:00 pm Pacific time) for an emergency inquiry, please contact Apple’s Global Security Operations Center (GSOC) at 001 408 974-2095. This phone number offers language support for multiple languages.

E. Account Restriction/Deletion Requests

In the event that government or law enforcement is requesting that Apple restrict/delete a customer’s Apple ID, Apple requires a court order or other equivalent domestic legal process (including conviction or warrant) demonstrating the account to be restricted/deleted was used unlawfully or in violation of Apple’s terms of service. Apple will not restrict/delete a customer’s account on receipt of an unofficial/ invalid request.

Apple carefully reviews all requests from government and law enforcement to ensure there’s a valid legal basis for each request. In instances where Apple determines there is no valid legal basis or where the court order does not demonstrate that the account to be restricted/deleted was used unlawfully or in violation of Apple’s terms of service, Apple will reject/challenge the request.

Where Apple receives a satisfactory court order or other equivalent domestic legal process (including conviction or warrant) from government or law enforcement demonstrating that the account to be restricted/deleted was used unlawfully or in violation of Apple’s terms of service, Apple will take the requisite action to restrict/delete the account in compliance with the court order; and advise the requesting agent accordingly.

F. User Notice

Apple will notify customers/users when their Apple account information is being sought in response to a valid legal request from government or law enforcement, except where providing notice is explicitly prohibited by the valid legal request, by a court order Apple receives, by applicable law or where Apple, in its sole discretion, believes that providing notice creates a risk of injury or death to an identifiable individual, in situations where the case relates to child endangerment, or where notice is not applicable to the underlying facts of the case, or where Apple reasonably considers that to do so would likely pervert the course of justice or prejudice the administration of justice.

After 90 days Apple will provide delayed notice for emergency disclosure requests except where notice is prohibited by court order or applicable law or where Apple, in its sole discretion, believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals or in situations where the case relates to child endangerment. Apple will provide delayed notice for

requests after expiration of the non-disclosure period specified in a court order unless Apple, in its sole discretion, reasonably believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals, in situations where the case relates to child endangerment, or where notice is not applicable to the underlying facts of the case, or where Apple reasonably considers that to do so would likely pervert the course of justice or prejudice the administration of justice.

Apple will notify its customers when their Apple account has been restricted/deleted as a result of Apple receiving a court order (including conviction or warrant) demonstrating that the account to be restricted/deleted was used unlawfully or in violation of Apple's terms of service; except where providing notice is prohibited by the legal process itself, by a court order Apple receives, by applicable law, in situations where the case relates to child endangerment, or where Apple, in its sole discretion, reasonably believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals, or where notice is not applicable to the underlying facts of the case, or where Apple reasonably considers that to do so would likely pervert the course of justice or prejudice the administration of justice.

III. Information Available from Apple

This section covers the general types of information which may be available from Apple at the time of the publishing of these Guidelines.

A. Device Registration

Basic registration or customer information, including, name, address, email address, and telephone number is provided to Apple by customers when registering an Apple device prior to iOS 8 and Mac OS Sierra 10.12. Apple does not verify this information, and it may not be accurate or reflect the device's owner. Registration information for devices running iOS 8 and later versions, as well as Macs running Mac OS Sierra 10.12 and later versions is received when a customer associates a device to an iCloud Apple ID. This information may not be accurate or reflect the device's owner. Registration information, if available, may be obtained with the appropriate legally valid request for the requestor's country.

Please note, Apple device serial numbers do not contain the letters "O" or "I," rather Apple utilises the numbers 0 (zero) and 1 (one) in serial numbers. Requests for serial numbers with either the letter "O" or "I" will yield no results.

B. Customer Service Records

Contacts that customers have had with Apple customer service regarding a device or service may be obtained from Apple. This information may include records of support interactions with customers regarding a particular Apple device or service. Additionally, information regarding the device, warranty, and repair may also be available. This information, if available, may be obtained with the appropriate legally valid request for the requestor's country.

C. iTunes

iTunes is a free software application which customers use to organize and play digital music and video on their computers. It's also a store that provides content for customers to download for their computers and iOS devices. When a customer opens an iTunes account, basic subscriber information such as name, physical address, email address, and telephone number can be provided by the customer. Additionally, information regarding iTunes purchase/download transactions and connections, update/re-download connections, and iTunes Match connections may also be available. iTunes subscriber information and connection logs with IP addresses, if available, may be obtained with the appropriate legally valid request for the requestor's country.

Requests for iTunes data must include the Apple device identifier (serial number, IMEI, MEID, or GUID) or relevant Apple ID/account email address. If the Apple ID/account email address are unknown, it is necessary to provide Apple with iTunes subscriber information in the form of full name **and** phone number, and/or full name **and** physical address in order to identify the subject iTunes subscriber account. Government or law enforcement officers may also provide a valid iTunes order number or a complete debit or credit card number associated with the iTunes purchase(s). A customer name in combination with these parameters may also be provided, but customer name alone is insufficient to obtain information.

D. Apple Retail Store Transactions

Point of Sale transactions are cash, credit/debit card, or gift card transactions that occur at an Apple Retail Store. Requests for Point of Sale records must include the complete credit/debit card number used and may also include additional information such as date and time of transaction, amount, and items purchased. Information regarding the type of card associated with a particular purchase, name of the purchaser, email address, date/time of the transaction, amount of the transaction, and store location, if available, may be obtained with the appropriate legally valid request for the requestor's country.

Requests for duplicate copies of receipts must include the retail transaction number associated with the purchase(s) and, if available, they may be obtained with the appropriate legally valid request for the requestor's country.

E. Apple Online Store Purchases

Apple maintains information regarding Apple Online Store purchases, which may include name of the purchaser, shipping address, telephone number, email address, product(s) purchased, purchase amount, and IP address of the purchase. Requests for information pertaining to Apple Online Store orders must include a complete credit/debit card number or an order number, reference number, or serial number of the item purchased. A customer name in combination with these parameters may also be provided, however customer name alone is insufficient to obtain information. Alternatively, requests for information pertaining to Apple Online Store orders may include the relevant Apple ID/account email address. If the Apple ID/account email address are unknown, Apple requires subscriber information in the form of full name **and** phone number, and/or full name **and** physical address to identify the subject Apple account. Apple Online Store purchase information, if available, may be obtained with a legally valid request for the requestor's country.

F. Gift Cards

Apple Store gift cards and iTunes Store gift cards have both a serial number and a PIN code (also known as redemption PIN code). Apple Store gift cards and iTunes Store gift cards have multiple serial number formats depending on variables such as design and/or date of issue. The redemption PIN codes permit the holder of either gift card type to access the funds on the gift card. The PIN code of the gift card is the most reliable parameter for Apple to search for information related to the gift card. In instances where a legal request contains 5 or more gift card PIN codes, Apple requests these gift card PIN codes to also be submitted in editable electronic format.

i. Apple Store Gift Cards

Apple Store gift cards may be used for purchases in either the Apple Online Store or an Apple Retail Store. The PIN code on an Apple Store gift card starts with the letter 'Y'. In some instances, older Apple Store gift cards may contain a PIN code format that is 8 digits. Available records may include gift card purchaser information (if purchased from Apple as opposed to a third-party merchant), associated purchase transactions, and items purchased. In some instances, Apple may be able to cancel or suspend an Apple Store gift card, depending on the status of the specific card. Apple Store gift card information, if available, may be obtained with the appropriate legally valid request for the requestor's country.

ii. iTunes Store Gift Cards

iTunes Store gift cards can be used in the iTunes Store, App Store, iBooks Store and Mac App Store. The PIN code on an iTunes Store gift card starts with the letter 'X'. With the PIN code, Apple can determine whether the iTunes Store gift card has been activated (purchased at a retail point-of-sale) or redeemed (added to the store credit balance of an iTunes account).

When an iTunes Store gift card is activated, available records may include the name of the store, location, date, and time. When an iTunes Store gift card is redeemed, available records may include subscriber information for the related iTunes account, date and time of activation and/or redemption, and redemption IP address. In some instances, Apple may be able to disable an iTunes Store gift card, depending on the status of the specific card. iTunes Store gift card information, if available, may be obtained with the appropriate legally valid request for the requestor's country.

G. iCloud

iCloud is Apple's cloud service that allows users to access their music, photos, documents, and more from all their devices. iCloud also enables subscribers to back up their iOS devices to iCloud. With the iCloud service, subscribers can set up an iCloud.com email account. iCloud email domains can be @icloud.com, @me.com and @mac.com. All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its U.S. data centres.

iCloud is a subscriber based service. Requests for iCloud data must include the relevant Apple ID/ account email address. If Apple ID/account email address are unknown, Apple requires subscriber

information in the form of full name and phone number, and/or full name and physical address to identify the subject Apple account.

The following information may be available from iCloud:

i. Subscriber information

When a customer sets up an iCloud account, basic subscriber information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. iCloud subscriber information and connection logs with IP addresses, if available, may be obtained with the appropriate legally valid request for the requestor's country. Connection logs are retained up to 30 days.

ii. Mail Logs

iCloud mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. iCloud mail logs are retained up to 60 days; and, if available, may be obtained with the appropriate legally valid request for the requestor's country.

iii. Email Content and Other iCloud Content. My Photo Stream, iCloud Photo Library, iCloud Drive, Contacts, Calendars, Bookmarks, Safari Browsing History, iOS Device Backups

iCloud stores content for the services that the subscriber has elected to maintain in the account while the subscriber's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. iCloud content may include email, stored photos, documents, contacts, calendars, bookmarks, Safari browsing history and iOS device backups. iOS device backups may include photos and videos in the Camera Roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail. All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its U.S. data centres.

All requests from government and law enforcement agencies outside of the United States for content stored in our data centers in the United States, with the exception of emergency circumstances (defined above in Emergency Requests), must comply with the United States Electronic Communications Privacy Act (ECPA). A request under a Mutual Legal Assistance Treaty or Agreement with the United States is in compliance with ECPA. Apple Inc. will provide subscriber content, as it exists in the subscriber's account, only in response to such legally valid process.

H. Find My iPhone

Find My iPhone is a user-enabled feature by which an iCloud subscriber is able to locate his/her lost or misplaced iPhone, iPad, iPod touch, Apple Watch or Mac and/or take certain actions, including putting the device in lost mode, or locking or wiping the device. More information about this service can be found at http://www.apple.com/icloud/find-my-iphone.html.

For the Find My iPhone feature to work for a user who has lost their device, it must have already been enabled on that specific device before it was lost. The Find My iPhone feature on a device cannot be activated after the device has been lost, or remotely, or upon a request from government or law enforcement. Device location services information is stored on each individual device and Apple cannot retrieve this information from any specific device. Location services information for a device located through the Find My iPhone feature is user facing and Apple does not have content of maps or alerts transmitted through the service. The following support link provides information and steps that can be taken by a user if an iOS device is lost or stolen: http://support.apple.com/en-us/HT201472.

Find My iPhone connection logs are available for a period of approximately 30 days; and, if available, may be obtained with the appropriate legally valid request for the requestor's country. Find My iPhone transactional activity for requests to remotely lock or erase a device, if available, may be obtained with the appropriate legally valid request for the requestor's country.

I. Extracting Data from Passcode Locked iOS Devices

For all devices running iOS 8.0 and later versions, Apple is unable to perform an iOS device data extraction as the data typically sought by law enforcement is encrypted, and Apple does not possess the encryption key. All iPhone 6 and later device models are manufactured running iOS 8.0 or a later version of iOS.

For devices running iOS 4 through iOS 7, Apple may, depending on the status of the device, perform iOS data extractions, pursuant to California's Electronic Communications Privacy Act (CalECPA, California Penal Code sections 1546-1546.4). In order for Apple to perform an iOS data extraction for a device that meets these criteria, law enforcement should obtain a search warrant issued upon a showing of probable cause under CalECPA. Apart from CalECPA, Apple has not identified any established legal authority which requires Apple to extract data as a third-party in a law enforcement investigation.

J. Other Available Device Information

MAC Address: A Media Access Control address (MAC address), is a unique identifier assigned to network interfaces for communications on the physical network segment. Any Apple product with network interfaces will have one or more MAC addresses, such as Bluetooth, Ethernet, Wi-Fi, or FireWire. By providing Apple with a serial number (or in the case of an iOS device, IMEI, MEID, or UDID), responsive information, if available, may be obtained with the appropriate legally valid request for the requestor's country.

UDID: The unique device identifier (UDID) is a sequence of 40 letters and numbers that is specific to a particular iOS device. It will look similar to the following: 2j6f0ec908d137be2e1730235f5664094b831186. If government or law enforcement is in possession of the device, the device may be connected to iTunes

in order to obtain the UDID. Under the iTunes summary tab, the UDID can be revealed by clicking on the serial number.

K. Requests for Apple Retail Store CCTV Data

CCTV data may vary by store location. CCTV data is typically maintained at an Apple retail store for a maximum of 30 days. In many jurisdictions it is as short as twenty-four (24) hours taking account of local laws. After this time frame has passed, data may not be available. A request for CCTV data can be made at any local Apple retail store. Government or law enforcement should provide specific date, time, and related transaction information regarding the data requested.

L. Game Center

Game Center is Apple's social gaming network. Information regarding Game Center connections for a user or a device may be available. Connection logs with IP addresses and transactional records, if available, may be obtained with the appropriate legally valid request for the requestor's country.

M. iOS Device Activation

When a customer activates an iOS device or upgrades the software, certain information is provided to Apple from the service provider or from the device, depending on the event. IP addresses of the event, ICCID numbers, and other device identifiers may be available. This information, if available, may be obtained with the appropriate legally valid request for the requestor's country.

N. Sign-on Logs

Sign-on activity for a user or a device to Apple services such as iTunes, iCloud, My Apple ID, and Apple Discussions, when available, may be obtained from Apple. Connection logs with IP addresses, if available, may be obtained with the appropriate legally valid request for the requestor's country.

O. My Apple ID and iForgot Logs

My Apple ID and iForgot logs for a user may be obtained from Apple. My Apple ID and iForgot logs may include information regarding password reset actions. Connection logs with IP addresses, if available, may be obtained with the appropriate legally valid request for the requestor's country.

P. FaceTime

FaceTime communications are end-to-end encrypted and Apple has no way to decrypt FaceTime data when it is in transit between devices. Apple cannot intercept FaceTime communications. Apple has FaceTime call invitation logs when a FaceTime call invitation is initiated. These logs do not indicate that any communication between users actually took place. FaceTime call invitation logs are retained up to 30 days. FaceTime call invitation logs, if available, may be obtained with a court order, warrant or domestic equivalent.

Q. iMessage

iMessage communications are end-to-end encrypted and Apple has no way to decrypt iMessage data when it is in transit between devices. Apple cannot intercept iMessage communications and Apple does not have iMessage communication logs. Apple does have iMessage capability query logs. These logs indicate that a query has been initiated by a device application (which can be Messages, Contacts, Phone, or other device application) and routed to Apple's servers for a lookup handle (which can be a phone number, email address, or Apple ID) to determine whether that lookup handle is "iMessage capable." iMessage capability query logs do not indicate that any communication between users actually took place. Apple cannot determine whether any actual iMessage communication took place on the basis of the iMessage capability query logs. Apple also cannot identify the actual application that initiated the query. iMessage capability query logs do not confirm that an iMessage event was actually attempted. iMessage capability query logs are retained up to 30 days. iMessage capability query logs, if available, may be obtained with a court order, warrant or domestic equivalent.

IV. Frequently Asked Questions

Q: Can I email Apple with questions regarding my law enforcement information request?
A: Yes, questions or inquiries regarding your law enforcement information request should be emailed to the relevant mailbox for your country/region, as outlined in this document.

Q: Does a device have to be registered with Apple in order to function or be used?
A: No, a device does not have to be registered with Apple in order for it to function or be used.

Q: Can Apple provide me with the passcode of an iOS device that is currently locked?
A: No, Apple does not have access to a user's passcode.

Q: Can you help me return a lost or stolen device to the rightful owner?
A: In cases where you as a government or law enforcement officer outside of the United States has recovered a suspected lost or stolen device and want to return it to the "original owner," you should forward your request to the relevant mailbox for your country/region, as outlined in this document, and include the device's serial or IMEI number and any additional relevant information. If registration information is available, we will contact the registrant and advise him or her to contact you.

Q: Does Apple keep a list of lost or stolen devices?
A: No, Apple does not keep a list of lost or stolen devices.

Q: What should be done with response information when law enforcement has concluded the investigation/criminal case?
A: Information and data provided to government or law enforcement containing personally identifiable information (including any copies made) should be destroyed after the related investigation, criminal case, and all appeals have been fully exhausted.

Q: Do you notify users of receiving law enforcement information requests in relation to them?
A: Yes, Apple's notice policy applies to account requests from law enforcement, government and private parties. Apple will notify customers and account holders unless there is a non-disclosure order or applicable law prohibiting notice, or where Apple, in its sole discretion, reasonably believes that such notice may pose immediate risk of serious injury or death to a member of the public, the case relates to a child endangerment matter, or where notice is not applicable to the underlying facts of the case, or where it reasonably considers that to do so would likely pervert the course of justice or prejudice the administration of justice.