



# Legal Process Guidelines

## Government & Law Enforcement within the United States

These guidelines are provided for use by government and law enforcement agencies within the United States when seeking information from Apple Inc. (“Apple”) about users of Apple’s devices, products and services. Apple will update these Guidelines as necessary.

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 requests made by government and law enforcement agencies outside the United States to Apple’s relevant local entities.

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. For all requests from government and law enforcement agencies within the United States for content, with the exception of emergency circumstances (defined in the Electronic Communications Privacy Act 1986, as amended), Apple will only provide content in response to a search warrant issued upon a showing of probable cause.

For private party requests Apple complies with the laws pertaining to 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**

### **II. Service of Legal Process**

- A. Government, Law Enforcement, and Private Party Subpoenas, Search Warrants, and Court Orders
- B. Managing and Responding to Government, Law Enforcement, and Private Party Subpoenas, Search Warrants, and Court Orders
- C. Witness Testimony Subpoenas
- D. Preservation Requests
- E. Emergency Requests
- F. Account Restriction/Deletion Requests
- G. User Notice

### **III. Information Available from Apple**

- A. Device Registration
- B. Customer Service Records
- C. iTunes
- D. Apple Retail Store Transactions
- E. Apple Online Store Purchases
- F. Gift Cards
- G. iCloud
- H. Find My iPhone
- I. Extracting Data from Passcode Locked iOS Devices
- J. Other Available Device Information
- K. Requests for Apple Retail Store CCTV Data
- L. Game Center
- M. iOS Device Activation
- N. Sign-on Logs
- O. My Apple ID and iForgot Logs
- P. FaceTime
- Q. iMessage

### **IV. Frequently Asked Questions**

## 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 within the United States regarding the legal process that Apple requires in order to disclose electronic information to government and law enforcement agencies within 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 [lawenforcement@apple.com](mailto:lawenforcement@apple.com).

The above mailbox is intended solely for use by law enforcement and government personnel. If you choose to send an email to this address, it must be from a valid and official government or law enforcement email address.

The majority of subpoenas, search warrants, and court orders 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 legal process to avoid misinterpretation, challenge and/or rejection in response to an unclear, inappropriate, or over-broad request. With the exception of emergency circumstances (defined in the Electronic Communications Privacy Act 1986, as amended), a search warrant issued upon a probable cause showing is required when government and law enforcement are requesting user content.

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. Service of Legal Process**

### **A. Government, Law Enforcement, and Private Party Subpoenas, Search Warrants, and Court Orders**

Apple accepts service of subpoenas, search warrants, and court orders 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 submitting a legal request to Apple should transmit it directly from their official government or law enforcement email address to mailbox: [lawenforcement@apple.com](mailto:lawenforcement@apple.com).

The above mailbox is intended solely for use by government and law enforcement personnel. When government or law enforcement has served legal process on Apple by email to [lawenforcement@apple.com](mailto:lawenforcement@apple.com), there is no need to serve duplicate hardcopy process on Apple by mail. 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.

Note: All matters that are not government or law enforcement related must be either personally served at Apple's headquarters: One Apple Park Way, Cupertino, California, 95014; or served through CT Corporation (Apple's registered agent for service of process).

For inquiries related to law enforcement legal process, please contact: [lawenforcement@apple.com](mailto:lawenforcement@apple.com). If you are inquiring regarding the status of a specific subpoena, search warrant, or court order, please do not contact Apple until at least 10 business days after service of your request unless the matter involves imminent harm or threat to life.

### **B. Managing and Responding to Government, Law Enforcement, and Private Party Subpoenas, Search Warrants, and Court Orders**

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. Witness Testimony Subpoenas**

Apple will not waive service requirements for subpoenas seeking witness testimony nor accept service via electronic means. All subpoenas seeking witness testimony must either be personally served on Apple or served through Apple's registered agent for service of process. Apple will resist subpoenas for witness testimony that are served with fewer than 14 days advance notice.

## D. Preservation Requests

Requests to preserve information pursuant to 18 U.S.C. § 2703(f) should be transmitted directly from an official government or law enforcement email address to the mailbox: [lawenforcement@apple.com](mailto:lawenforcement@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 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 for one additional 90-day period upon receipt of 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 will not preserve new material in response to such requests.

## E. Emergency Requests

The Electronic Communications Privacy Act (“ECPA”) covers the authorized disclosure of content by Apple. An exception to the requirement that government or law enforcement obtain a search warrant for customer content is provided by ECPA in situations in which the case involves an emergency. Under 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4) Apple is permitted, but not required, to voluntarily disclose information, including contents of communications and customer records, to a federal, state, or local governmental entity if Apple believes in good faith that an emergency involving imminent danger of death or serious physical injury to any person requires such disclosure without delay.

In order to request that Apple voluntarily disclose information on an emergency basis, 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](mailto: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 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 (408) 974-2095.

## F. Account Restriction/Deletion Requests

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

Apple carefully reviews all requests from government, law enforcement and private parties 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, Apple will reject/challenge the request.

Where Apple receives a satisfactory court order (including conviction or warrant) from government, law enforcement or private party demonstrating that the account to be restricted/deleted was used unlawfully, Apple will take the requisite action to restrict/delete the account in compliance with the court order; and advise the requesting agent/party accordingly.

## **G. User Notice**

Apple will notify customers/users when their Apple account information is being sought in response to legal process from government, law enforcement, or third parties, except where providing notice is explicitly prohibited by the legal process itself, by a court order Apple receives (e.g., an order under 18 U.S.C. §2705(b)), 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.

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.

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 (e.g., an order under 18 U.S.C. §2705(b)), 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.

If Apple receives a National Security Letter (NSL) from the U.S. government that contains an indefinite gag order, Apple will notify the government that it would like the court to review the nondisclosure provision of the NSL pursuant to the USA FREEDOM Act of 2015. The government then has 30 days to let the court know why the nondisclosure should remain in effect or can let Apple know that the nondisclosure no longer applies. If Apple receives notice that the nondisclosure no longer applies, it will notify the affected customer(s) pursuant to Apple's customer notice policies.

### 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 a subpoena or greater legal process.

Please note, Apple device serial numbers do not contain the letters "O" or "I," rather Apple utilizes 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 a subpoena or greater legal process.

#### 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 can be obtained with a subpoena or greater legal process. iTunes purchase/download transactional records and records of the specific content purchased or downloaded, if available, may be obtained with an order under 18 U.S.C. § 2703(d) or a court order with the equivalent legal standard or a search warrant.

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.



**Please note:** where your legal request contains full credit/debit card data, for data security purposes, the credit/debit card data should be transmitted in a password-protected/encrypted document/file to [lawenforcement@apple.com](mailto:lawenforcement@apple.com) and the password should be transmitted in a separate email.

#### **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 a subpoena or greater legal process.

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 a subpoena or greater legal process.

**Please note:** where your legal request contains full credit/debit card data, for data security purposes, the credit/debit card data should be transmitted in a password-protected/encrypted document/file to [lawenforcement@apple.com](mailto:lawenforcement@apple.com) and the password should be transmitted in a separate email.

#### **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 subpoena or greater legal process.

**Please note:** where your legal request contains full credit/debit card data, for data security purposes, the credit/debit card data should be transmitted in a password-protected/encrypted document/file to [lawenforcement@apple.com](mailto:lawenforcement@apple.com) and the password should be transmitted in a separate email.

#### **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. Apple can provide available information regarding Apple Store gift cards or iTunes Store gift cards in response to a subpoena or greater legal process. 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 a subpoena or greater legal process.

**Please note:** where your legal request contains full Apple Store gift card data, for data security purposes, the Apple Store gift card data should be transmitted in a password-protected/encrypted document/file to [lawenforcement@apple.com](mailto:lawenforcement@apple.com) and the password should be transmitted in a separate email.

**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 a subpoena or greater legal process.

**Please note:** where your legal request contains full iTunes Store gift card data, for data security purposes, the iTunes Store gift card data should be transmitted in a password-protected/encrypted document/file to [lawenforcement@apple.com](mailto:lawenforcement@apple.com) and the password should be transmitted in a separate email.

## 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 centers.

iCloud is a subscriber based service. Requests for iCloud data must 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.

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 a subpoena or greater legal process. Connection logs are retained up to 30 days.

### **ii. Mail Logs**

Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. Mail logs, if available, may be obtained with a court order under 18 U.S.C. § 2703(d) or a court order with an equivalent legal standard or a search warrant. iCloud mail logs are retained up to 30 days.

### **iii. Email Content and Other iCloud Content. My Photo Stream, iCloud Photo Library, iCloud Drive, Contacts, Calendars, Bookmarks, Safari Browsing History, Maps Search History, Messages, 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, Maps Search History, Messages and iOS device backups. iOS device backups may include photos and videos in the Camera Roll, device settings, app data, iMessage, Business Chat, 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 centers. iCloud content, as it exists in the subscriber's account, may be provided in response to a search warrant issued upon a showing of probable cause.

## **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 a subpoena or greater legal process. Find My iPhone transactional activity for requests to remotely lock or erase a device, if available, may be obtained with an order under 18 U.S.C. § 2703(d) or a court order with the equivalent legal standard or a search warrant.

## **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 a subpoena or greater legal process.

## **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. After this timeframe has passed, data may not be available. Requests which are solely for CCTV data can be sent to the mailbox: [lossprevention@apple.com](mailto:lossprevention@apple.com). 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, if available, may be obtained with a subpoena or greater legal process. Game Center transactional records and/or records of the specific games accessed, if available, may be obtained with an order under 18 U.S.C. §2703(d) or a court order with the equivalent legal standard or a search warrant.

## **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 a subpoena or greater legal process.

**Dual SIM:** For devices featuring Dual SIM, carrier information for the nano SIM and/or eSIM, if available, may be obtained with a subpoena or greater legal process. An eSIM is a digital SIM that allows users to activate a cellular plan from a carrier without having to use a physical nano-SIM. More information can be found at <http://support.apple.com/en-us/HT209044>.

## **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 a subpoena or greater legal process.

## **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 a subpoena or greater legal process. Transactional records, if available, may be obtained with an order under 18 U.S.C. §2703(d) or court order with the equivalent legal standard or search warrant.

## **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 an order under 18 U.S.C. §2703(d) or court order with the equivalent legal standard or search warrant.

## **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 an order under 18 U.S.C. §2703(d) or court order with the equivalent legal standard or search warrant.

## IV. Frequently Asked Questions

**Q: Can I email Apple with questions regarding my legal process?**

A: Yes, questions or inquiries regarding government legal process can be emailed to [lawenforcement@apple.com](mailto:lawenforcement@apple.com).

**Q: I need to personally serve Apple, where should I go?**

A: All personal service can be made at Apple's Cupertino, California headquarters located at the following address:

Apple Inc.  
One Apple Park Way  
Cupertino, CA 95014

**Q: Can I serve a deposition subpoena directly on an Apple retail store?**

A: No, all subpoenas for testimony, including subpoenas for deposition or trial testimony, need to be personally served on Apple as specified above.

**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 person who lost it?**

A: In these cases, contact [lawenforcement@apple.com](mailto:lawenforcement@apple.com). Please include the device's serial number in your email and any additional pertinent information. If customer information is available, Apple will contact the customer and instruct him or her to contact law enforcement to recover the device. However, if the customer cannot be determined from available information you may be instructed to submit a subpoena or other valid legal request.

**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 the produced files and records 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 legal process?**

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.

**Q: Can Apple intercept users' communications pursuant to a Wiretap Order?**

A: Apple can intercept users' email communications, upon receipt of a valid Wiretap Order. Apple cannot intercept users' iMessage or FaceTime communications as these communications are end-to-end encrypted.

**Q: I am looking into whether a user's email reach the requirements for interstate commerce. Where are the iCloud email servers located?**

A: Apple's U.S. email servers are located in Arizona, California, Nevada, North Carolina, and Oregon.

**Q: I requested information in the body of my email, why was it not provided?**

A: Requests for information not included within the body of the signed subpoena, search warrant, or court order will be disregarded; Apple will only provide information that is specified in the actual executed legal process document.