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 entities in the relevant region or country about customers 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 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.com and Apple Media Services 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 customer data related to Apple services within their respective regions.

All other requests for information regarding Apple customers, including customer 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, with the exception of emergency circumstances (defined below in Emergency Requests), must comply with applicable laws, including the United States Electronic Communications Privacy Act (ECPA). A request under a Mutual Legal Assistance Treaty or under an Executive Agreement under the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act Agreement") is in compliance with ECPA. Apple will provide customer content, as it exists in the customer's account, only in response to such legally valid process.

For private party requests, Apple complies with the laws pertaining to local entities that control customer 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 objected, challenged or rejected.

Apple provides responses to the requesting law enforcement agency at the official law enforcement email address of the requesting officer. All evidence preservation pursuant to the responses provided by Apple is the responsibility of the requesting law enforcement agency.

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 touch, Apple TV, Apple TV+, Apple Watch, HomePod, AirPods, AirTag a portfolio of consumer and professional software applications, the iOS and macOS X operating systems, iCloud, and a variety of accessory, service and support offerings. Apple also sells and delivers digital content and applications through Apple Music, App Store, Apple Books, and Mac App Store. Customer information is held by Apple in accordance with Apple's privacy policy and the applicable terms of service for the particular service offering. Apple is committed to maintaining the privacy of the customers of Apple products and services ("Apple customers"). Accordingly, other than in emergency situations as provided by law, information about Apple customers 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 lawenforcement@apple.com.

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

Legal requests to Apple should 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, objection, 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, with the exception of emergency circumstances (defined below in Emergency Requests), must comply with applicable laws including the United States Electronic Communications Privacy Act (ECPA). A request under a Mutual Legal Assistance Treaty or under an Executive Agreement under the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act Agreement") is in compliance with ECPA. Apple will provide customer content, as it exists in the customer's account, only in response to such legally valid process.

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 requesting government or law enforcement agency. 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 lawenforcement@apple.com.

The above mailbox is intended solely for use by government and law enforcement personnel. Where requests contain 5 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 (example Numbers, Excel, Pages or Word document). Identifiers such as these are generally required in order to conduct searches for information related to devices, accounts, or financial transactions.

Please Note: Apple will not download legal requests or related documents from any link submitted in an email due to system security standards.

In order for Apple to disclose customer information in response to a request from law enforcement, it is necessary for the requesting officer to indicate the legal basis which authorises the collection of evidential information in the form of personal data by a law enforcement agency from a Data Controller such as Apple. Examples of requests Apple considers to be legally valid are: Production Orders (Australia, Canada, New Zealand), Requisition or Judicial Rogatory Letters (France), Solicitud Datos (Spain), Ordem Judicial (Brazil), Auskunftsersuchen (Germany), Obligation de dépôt (Switzerland), 個人情報の開示依頼 (Japan), Personal Data Request, Orders, Warrants and Communications Data Authorisations (U.K.), as well as equivalent court orders and/or requests from other countries.

B. Managing and Responding to Government and Law Enforcement Information Requests

Apple carefully reviews all legal requests to ensure that there's a valid legal basis for each request; and complies with legally valid requests. Where Apple determines that there is no valid legal basis or where a request is unclear, inappropriate or over-broad, Apple will object, challenge or reject the request.

For processing purposes and due to system limitations, Apple cannot accept legal requests that contain more than 25 account identifiers. If law enforcement submits legal requests with more than 25 account identifiers, Apple will respond to the first 25 and law enforcement will need to resubmit new legal request for any additional identifiers.

C. Preservation Requests

All requests from government and law enforcement agencies outside of the United States for content, with the exception of emergency circumstances (defined below in Emergency Requests), must comply with applicable laws, including the United States Electronic Communications Privacy Act (ECPA). A

request under a Mutual Legal Assistance Treaty or under an Executive Agreement under the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act Agreement") is in compliance with ECPA. A request to preserve data in advance of impending ECPA compliant request should be sent by email to 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 customer of the subject Apple account. When a preservation request has been received, Apple will preserve a one-time data pull of the requested existing customer 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. An attempt to serve more than two preservation requests for the same account will result in the second request being treated as a request for an extension of the original preservation, and not a separate preservation of new data.

D. Emergency Requests

Apple considers a request to be an emergency request when it relates to circumstances involving imminent and serious threats to the life/safety of individuals; the security of a State; or the security of critical infrastructure/installations.

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

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 exigent@apple.com with the words "Emergency Request" in the subject line.

If a government or law enforcement agency seeks 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 a government or law enforcement agency needs to reach Apple 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

If a government or law enforcement agency requests that Apple restrict/delete a customer's Apple ID, Apple requires a court order or other equivalent domestic legal process (often a judgment of conviction or warrant) demonstrating the account to be restricted/deleted was used unlawfully.

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, Apple will reject/challenge the request.

Where Apple receives a satisfactory court order or other equivalent domestic legal process (often a judgment of conviction or warrant) from government or law enforcement 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 accordingly.

F. Customer Notice

Apple will notify customers 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.

After 90 days Apple will provide delayed notice for emergency disclosures 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 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 (often a judgment of 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.

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 macOS 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 macOS 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. In instances where a legal request contains 5 or more serial numbers, Apple requests these serial numbers to also be submitted in editable electronic format (example Numbers, Excel, Pages or Word document).

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. Apple Media Services

App Store, Apple Music, Apple TV app, Apple Podcasts, and Apple Books ("Apple Media Services") are software applications which customers use to organize and play apps, digital music and video and stream content. Apple Media Services also provide content for customers to download for their computers and iOS devices. When a customer opens an Apple account, basic customer information such as name, physical address, email address, and telephone number can be provided by the customer. Additionally, information regarding Apple Media Service purchase/download transactions and connections, update/re-download connections may also be available. IP address information may be limited to the most recent 18 months. Apple Media Service customer 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 Apple Media Service 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 Apple Media Service customer information in the form of full name **and** phone number, and/or full name **and** physical address in order to identify the subject Apple Media Service customer account. Government or law enforcement officers may also provide a valid Apple Media Service order number or a complete debit or credit card number associated with the Apple Media Service 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 (.PDF and editable format, example Numbers, Excel, Pages or Word document) to lawenforcement@apple.com and the password should be transmitted in a separate email. Additionally Apple will not download legal request documents through any link provided in an email due to system security standards.

D. Apple Store Transactions

Point of Sale transactions are cash, credit/debit card, or gift card transactions that occur at an Apple 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.

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 (.PDF and editable format, example Numbers, Excel, Pages or Word document) to lawenforcement@apple.com and the password should be transmitted in a separate email. Additionally, Apple will not download legal request documents through any link provided in an email due to system security standards.

E. Apple.com Orders

Apple maintains information regarding orders online at Apple.com, 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 orders online at Apple.com must include a complete credit/debit card number or an order 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 orders online at Apple.com may include the relevant Apple ID/account email address. If the Apple ID/account email address are unknown, Apple requires customer information in the form of full name **and** phone number, and/or full name **and** physical address to identify the subject Apple account. Purchase information for orders online at Apple.com, if available, may be obtained with a legally valid request for the requestor's country.

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 (.PDF and editable format, example Numbers, Excel, Pages or Word document) to lawenforcement@apple.com and the password should be transmitted in a separate email. Additionally, Apple will not download legal request documents through any link provided in an email due to system security standards.

F. Gift Cards

Apple Store Gift Cards and App Store & iTunes Gift Cards have a serial number. These serial numbers have multiple formats depending on variables such as design and/or date of issue. Apple may provide available information regarding Apple Store Gift Cards and App Store & iTunes Gift Cards in response to the appropriate legally valid request for the requestor's country. In instances where a legal request contains 5 or more gift card serial numbers, Apple requests these gift card serial numbers to be transmitted in a password-protected/encrypted document (example Numbers, Excel, Pages or Word document) to lawenforcement@apple.com and the password should be transmitted in a separate email.

i. Apple Store Gift Cards

Apple Store Gift Cards may be used for purchases in either Apple.com or an Apple Store. 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.

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 (.PDF and editable format, example Numbers, Excel, Pages or Word document) to lawenforcement@apple.com and the password should be transmitted in a separate email. Additionally, Apple will not download legal request documents through any link provided in an email due to system security standards.

ii. App Store & iTunes Gift Cards

App Store & iTunes Gift Cards can be used in Apple Music, App Store, Apple Books and Mac App Store. With the serial number, Apple can determine whether the App Store & iTunes Gift Card has been activated (purchased at a retail point-of-sale) or redeemed (added to the store credit balance of an Apple account).

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

Please Note: Where your legal request contains full App Store & iTunes Gift Card data, for data security purposes, the App Store & iTunes Gift Card data should be transmitted in a password-protected/encrypted document (.PDF and editable format, example Numbers, Excel, Pages or Word document) to lawenforcement@apple.com and the password should be transmitted in a separate email. Additionally, Apple will not download legal request documents through any link provided in an email due to system security standards.

G. Apple Pay

Apple Pay transactions made at retail locations (e.g., for NFC/contactless communications) and in apps or online points-of-sale are authenticated securely on the customer's device and sent in encrypted form to the merchant or the merchant's payment processor. While transaction security is verified by an Apple server, Apple does not process payments or store such transactions nor the full credit/debit card numbers associated with purchases made using Apple Pay. This information may be available through the relevant issuing bank, the payment network, or the merchant.

More information about countries and regions that support Apple Pay can be found at https://support.apple.com/kb/HT207957.

To request transactional data for purchases made at Apple Store locations or through Apple.com, Apple requires the Device Primary Account Number (DPAN) used for the transaction. The DPAN is 16 digits and can be obtained from the issuing bank. Note: the DPAN is used in contactless payment transactions with the merchant in place of the actual credit/debit card number (FPAN/Funding PAN). The DPAN is converted into the corresponding FPAN by the payment processor. With the relevant DPAN information, Apple may be able to conduct a reasonable search to locate responsive information through its point-of-sale system. These records, if available, may be obtained with the appropriate legally valid request for the requestor's country.

Apple may be able to provide Apple Pay information regarding the type(s) of credit/debit card(s) a customer has added to Apple Pay along with customer information. This information, if available, may be obtained with the appropriate legally valid request for the requestor's country. To request such information, Apple would require a device identifier (Apple serial number, SEID, IMEI or MEID); or an Apple ID/account email address.

Please Note: Where your legal request contains the DPAN, for data security purposes, such data should be transmitted in a password-protected/encrypted document (.PDF and editable format, example Numbers, Excel, Pages or Word document) to lawenforcement@apple.com and the password should be transmitted in a separate email. Additionally, Apple will not download legal request documents through any link provided in an email due to system security standards.

H. iCloud

iCloud is Apple's cloud service that allows customers to access their photos, documents, and more from all their devices. iCloud also enables customers to back up their iOS and iPadOS devices to iCloud. With the iCloud service, customers 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. For data Apple can decrypt, Apple retains the encryption keys in its U.S. data centres. Apple does not receive or retain encryption keys for customer's end-to-end encrypted data.

iCloud is a customer 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 customer information in the form of full name **and** phone number, and/or full name **and** physical address to identify the subject Apple account. Where only a phone number or Apple ID/account email address are provided, available information for verified accounts associated with these criteria may be produced.

I. The following information may be available from iCloud:

I. Customer information

When a customer sets up an iCloud account, basic customer 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 customer 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 25 days.

II. Mail Logs

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 25 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, Maps Search History, Messages, iOS Device Backups

iCloud stores content for the services that the customer has elected to maintain in the account while the customer'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. For data Apple can decrypt, Apple retains the encryption keys in its U.S. data centres. Apple does not receive or retain encryption keys for customer's end-to-end encrypted data.

All requests from government and law enforcement agencies outside of the United States for content, with the exception of emergency circumstances (defined above in Emergency Requests), must comply with applicable laws, including the United States Electronic Communications Privacy Act (ECPA). A request under a Mutual Legal Assistance Treaty or under an Executive Agreement under the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act Agreement") is in compliance with ECPA. Apple will provide customer content, as it exists in the customer's account, only in response to such legally valid request.

II. Advanced Data Protection

Advanced Data Protection for iCloud is a feature that uses end-to-end encryption to protect iCloud data with Apple's highest level of data security. For users who enable Advanced Data Protection for iCloud, limited iCloud data may be available. More information on Advanced Data Protection can be found at https://support.apple.com/guide/security/advanced-data-protection-for-icloud-sec973254c5f/ web and https://support.apple.com/kb/HT212520.

The following information may be available from iCloud if a user has enabled Advanced Data Protection for iCloud:

a. Customer Information

When a customer sets up an iCloud account, basic customer 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 customer 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 25 days.

b. Mail Logs

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 25 days; and, if available, may be obtained with the appropriate legally valid request for the requestor's country.

c. Email Content and Other iCloud Content

For users that have enabled Advanced Data Protection, iCloud stores content for email, contacts, and calendars that the customer has elected to maintain in the account while the customer's account remains active. This data may be provided, as it exists in the customer's account, with the appropriate legally valid request for the requestor's country.

This limited data is stored by Apple and additionally encrypted at the location of the server. For data Apple can decrypt, Apple retains the encryption keys in its U.S. data centers. Apple does not receive or retain encryption keys for customer's end-to-end encrypted data.

Advanced Data Protection uses end-to-end encryption, and Apple cannot decrypt certain iCloud content, including Photos, iCloud Drive, Backup, Notes, and Safari Bookmarks. In some circumstances, Apple may retain limited information related to these iCloud services that may be obtained, if available, with the appropriate legally valid request for the requestor's country.

III. iCloud Private Relay

iCloud Private Relay is an internet privacy service offered as part of an iCloud+ subscription. Private Relay protects users' web browsing in Safari, DNS (Domain Name Space) resolution queries, and unencrypted http app traffic. Users must have an iCloud+ subscription and device with iOS 15, iPadOS 15, or macOS Monterey (macOS 12) or later to utilize iCloud Private Relay. More information about Private Relay can be found at https://support.apple.com/kb/HT212614 and https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF.

When Private Relay is enabled, user web browsing requests are sent through two separate, secure internet relays. User IP address is visible to user network provider and to the first relay, which is operated by Apple. User DNS records are encrypted, so neither party can see the address of the website the user is trying to visit. The second relay, which is operated by a third-party content provider, generates a temporary IP address, decrypts the name of the website user requested and connects user to the site. Private Relay validates that the client connecting is an iPhone, iPad, or Mac. Private Relay replaces the user's original IP address with one assigned from the range of IP addresses used by the service. The assigned relay IP address may be shared among more than one Private Relay user in the same area.

Where user web browsing requests utilize Private Relay, Apple is not able to determine the user client IP address or the corresponding user account from the Private Relay IP addresses. Apple has no information to provide regarding the AppleID associated with the Private Relay IP address

Note: iCloud Private Relay is not available in all countries or regions. If users have Private Relay enabled and travel somewhere Private Relay isn't available, it will automatically turn off and will turn on again when users re-enter a country or region that supports it.

I. Find My

Find My is a user-enabled feature by which an iCloud customer is able to locate his/her lost or misplaced iPhone, iPad, iPod touch, Apple Watch, AirPods, Mac, AirTag 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 https://www.apple.com/icloud/find-my/.

For the Find My feature to work for a customer who has lost their device, it must have already been enabled on that specific device before it was lost. The Find My feature on a device cannot be activated remotely, or after the device has been lost, or upon a request from a government or law enforcement agency. 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 feature is customer 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 customer if an iOS device is lost or stolen: http://support.apple.com/kb/HT201472.

Find My connection logs are available for a period up to 25 days; and, if available, may be obtained with the appropriate legally valid request for the requestor's country. Find My 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.

J. AirTag and Find My Network Accessory Program

The Find My app on iPhone, iPad, iPod touch, and Mac makes it easy for customers to locate personal items by attaching an AirTag or by using a product that is part of the Find My network accessory program.

With AirTag and iOS 14.5 and macOS 11.3 or later, customers may be assisted in finding missing personal items (keys, backpacks, luggage, etc.) using the Find My app. AirTag must be within Bluetooth range of the paired iPhone, iPad, or iPod touch in order to play a sound, or to use Precision Finding with compatible iPhone models. When not near its owner, the approximate location of AirTag may be provided if the AirTag is within range of a device in the Find My network, which is made up of hundreds of millions of Apple devices around the world. More information can be found at: https://support.apple.com/kb/HT212227 and https://support.apple.com/kb/HT210967.

The Find My network accessory program opens up the Find My network to third-party device manufacturer products (bikes, headphones, etc.) to utilize the service so customers can locate their supported third-party products with the Find My app with iOS 14.3 and macOS 11.1 or later.

To add AirTag or supported third-party products to the Items tab in the Find My app, customers must have an Apple ID, be signed into their iCloud account with Find My enabled, and register their AirTag or supported third-party products to their Apple ID. The interaction is end-to-end encrypted, and Apple cannot view the location of any AirTag or supported third-party products. More information can be found at https://support.apple.com/kb/HT211331.

With a serial number, Apple may be able to provide the paired account details in response to the appropriate legally valid request for the requestor's country. AirTag pairing history is available for a period up to 25 days. The following support link provides information on finding an AirTag serial number: https://support.apple.com/kb/HT211658.

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. In instances where a legal request contains 5 or more serial numbers, Apple

requests these serial numbers to also be submitted in editable electronic format (example Numbers, Excel, Pages or Word document).

K. 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 §§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.

L. IP Address Request

Before submitting legal process with an IP address as an identifier, Apple requests that law enforcement determine that the subject IP address is not a public or router IP address and not using Carrier-grade Network Address Translation (CGNAT) and confirm to Apple during service of the legal process that it is a non-public IP address. Moreover, such requests must include a date restriction of no more than three days. In response to such a request, Apple may be able to produce connection logs (see below, section III.Q) from which law enforcement can attempt to identify a particular Apple account/Apple ID to use as an identifier in a follow up legal process request. Apple customer data based on an IP address, if available, may be obtained with the appropriate legally valid request for the requestor's country.

M. 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 MAC address information, if available, may be obtained with the appropriate legally valid request for the requestor's country.

N. Requests for Apple Store CCTV Data

CCTV data may vary by store location. CCTV data is typically maintained at an Apple 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. Requests which are solely for CCTV data can be sent to lawenforcement@apple.com. Government or law enforcement should provide specific date, time, and related transaction information regarding the data requested.

O. Game Center

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

P. iOS Device Activation

When a customer activates an iOS device with a cellular service provider 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.

Dual SIM: For devices featuring Dual SIM, carrier information for the nano SIM and/or eSIM, if available, may be obtained with the appropriate legally valid request for the requestor's country. An eSIM is a digital SIM that allows customers 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/kb/HT209044. In China mainland, Hong Kong, and Macao, iPhone 12, iPhone 12 Pro, iPhone 12 Pro Max, iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max, iPhone XS Max, and iPhone XR feature Dual SIM with two nano- SIM cards.

Q. Connection Logs

Connection activity for a customer or a device to Apple services such as Apple Music, Apple TV app, Apple Podcasts, Apple Books, iCloud, My Apple ID, and Apple Discussions, when available, may be

obtained from Apple. These connection logs with IP addresses, if available, may be obtained with the appropriate legally valid request for the requestor's country.

R. My Apple ID and iForgot Logs

My Apple ID and iForgot logs for a customer 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.

S. 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 customers actually took place. FaceTime call invitation logs are retained up to 25 days. FaceTime call invitation logs, if available, may be obtained with the appropriate legally valid request for the requestor's country.

T. 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 customers 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 25 days. iMessage capability query logs, if available, may be obtained with the appropriate legally valid request for the requestor's country.

U. Apple TV app

The Apple TV app allows customers to browse, purchase, subscribe to, and play TV shows and movies from Apple TV+, Apple TV Channels, and third party apps and services. Purchase and download history, may be available.

Requests for Apple TV app customer 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 customer information in the form of full name and phone number, and/or full name and physical address in order to identify the subject customer account. Government or law enforcement officers may also provide a valid Apple order number or a complete credit/debit card number associated with an Apple TV app 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, such data should be transmitted in a password-protected/encrypted document (.PDF and editable format, example Numbers, Excel, Pages or Word document) to lawenforcement@apple.com and the password should be transmitted in a separate email. Additionally, Apple will not download legal request documents through any link provided in an email due to system security standards.

V. Sign in with Apple

Sign in with Apple is a more private way for customers to sign into third-party apps and websites using the customer's existing Apple ID. A Sign in with Apple button on a participating app or website allows a customer to set up an account and sign in with their Apple ID. Instead of using a social media account, or completing forms and selecting another new password, a customer can merely tap the Sign in with Apple button, review their information, and sign in quickly and securely with Face ID, Touch ID, or their device passcode. More information can be found at https://support.apple.com/kb/HT210318.

Hide My Email is a feature of Sign in with Apple. It uses Apple's private email relay service to create and share a unique, random email address that forwards emails to a customer's personal email address. Basic customer information can be obtained with the appropriate legally valid request for the requestor's country.

IV.Frequently Asked Questions

Q: Can I email Apple with questions regarding my law enforcement information request?
A: Yes, questions or inquiries regarding government legal process can be emailed to lawenforcement@apple.com.

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 customer'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. Please include the device serial number (or IMEI, if applicable) in your email and any additional relevant information. Information on finding the serial number is available here: https://support.apple.com/kb/HT204308.

If customer information is available, Apple will contact the customer and provide details 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 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 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 customers 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.