Recommandations concernant les procédures judiciaires

Application de la loi dans la région EMEIA

Ces recommandations sont destinées aux autorités chargées de l'application de la loi et autres organismes administratifs dans la région géographique EMEIA (Europe, Moyen-Orient, Inde, Afrique) sollicitant des informations sur des utilisateurs de produits ou services Apple auprès des entités concernées d'Apple qui fournissent des services dans cette région, ou à partir d'appareils Apple. Dans ces recommandations, Apple désignera la filiale responsable des informations clients dans une région particulière, selon son Engagement de confidentialité disponible sur le site http://www.apple.com/legal/privacy/fr-ww/. Apple mettra à jour ces recommandations, le cas échéant. Cette version date du 29 septembre 2015.

Toutes les demandes d'informations concernant les utilisateurs d'Apple, y compris les questions des utilisateurs sur la divulgation d'informations, doivent être formulées sur la page https://www.apple.com/befr/privacy/contact/. Ces recommandations ne s'appliquent pas aux demandes effectuées par les autorités chargées de l'application de la loi auprès des filiales locales d'Apple Inc. ou d'Apple en dehors de la région géographique EMEIA.

Pour les demandes d'informations émanant du gouvernement, nous respectons les lois applicables aux entités mondiales qui contrôlent nos données et fournissons les informations requises au titre de la loi. Pour les demandes de contenu provenant d'autorités chargées de l'application de la loi en dehors des États-Unis, sauf cas d'urgence (définis ci-dessous dans la partie « Demandes urgentes »), Apple ne fournit le contenu qu'en réponse à un mandat de perquisition émis conformément aux règles du Traité d'entraide judiciaire mutuelle ou dans le cadre d'autres efforts de coopération avec le Ministère de la Justice américain.

INDEX

I. Informations générales

Apple conçoit, fabrique et commercialise des appareils multimédias et de communication, des ordinateurs personnels, des lecteurs de musique numérique portables, et vend une diversité de logiciels, services, périphériques et solutions de mise en réseau, ainsi que des applications et du contenu numérique de tiers. Les produits et services d'Apple sont les suivants : Mac, iPhone, iPad, iPod, Apple TV, un portefeuille d'applications logicielles pour les particuliers et les professionnels, les systèmes d'exploitation iOS et Mac OS X, iCloud et une diversité d'offres d'accessoires, de services et d'assistance. Apple vend également des applications et du contenu numérique via l'iTunes Store, l'App Store, l'iBooks Store et le Mac App Store. Les informations sur les utilisateurs sont détenues par Apple conformément à son Engagement de confidentialité et aux conditions de service/conditions générales applicables à une offre de service donnée. Apple s'engage à respecter la vie privée des utilisateurs de produits et services Apple (« Utilisateurs Apple »). De la même manière, les informations sur les utilisateurs Apple ne seront pas divulguées sans une procédure judiciaire adéquate.

Ces recommandations sont conçues pour fournir des informations aux autorités chargées de l'application de la loi et aux organismes administratifs de la région EMEIA sur la procédure judiciaire exigée par Apple pour leur divulguer des informations électroniques. Elles n'ont pas pour objectif de fournir des conseils juridiques. La section Questions et réponses de ce document a pour but de répondre à certaines des questions les plus souvent reçues par Apple. Ni ces recommandations ni les Questions et réponses ne couvrent toutes les circonstances imaginables susceptibles de se produire. Par conséquent, veuillez nous contacter à l'adresse law.enf.emeia@apple.com pour toute autre question. Cette adresse e-mail est réservée exclusivement aux agents des autorités chargées de l'application de la loi et aux services administratifs. Si vous décidez d'envoyer un e-mail à cette adresse, le courrier doit provenir de l'adresse valide d'une autorité chargée de l'application de la loi ou d'un service administratif. Aucune disposition de ces recommandations n'a pour but de créer des droits juridiquement exécutoires contre Apple et les politiques d'Apple pourront être actualisées et modifiées à l'avenir sans en aviser les autorités chargées de l'application de la loi.

La plupart des demandes des autorités chargées de l'application de la loi reçues par Apple visent à obtenir des informations sur un client ou un appareil Apple particulier et sur les services spécifiques qu'Apple peut fournir à ce client. Apple peut fournir des informations sur un client ou un appareil Apple dans la mesure où Apple possède les informations requises conformément à ses politiques sur la conservation des données. Apple conserve les données comme il est indiqué dans la partie « Informations disponibles » ci-dessous. Toutes les autres données sont conservées pendant la période nécessaire pour répondre aux objectifs stipulés dans notre Engagement de confidentialité. Les autorités chargées de l'application de la loi doivent être aussi concises et spécifiques que possible dans l'établissement de leurs requêtes afin d'éviter toute interprétation erronée et/ou objection en réponse à une demande trop large.

II. Réponse à des procédures judiciaires

A. Demandes d'informations provenant des autorités

Apple accepte de répondre aux demandes d'informations légalement valides adressées par e-mail par les autorités chargées de l'application de la loi, sous réserve qu'elles soient transmises via l'adresse e-mail officielle de l'autorité concernée. Les agents des autorités chargées de l'application de la loi dans la région EMEIA qui soumettent une demande d'informations à Apple doivent remplir le formulaire « Demande d'informations pour une autorité chargée de l'application de la loi » figurant à l'annexe A et l'envoyer directement depuis leur adresse e-mail officielle

à law.enf.emeia@apple.com. Cette adresse e-mail d'Apple est réservée à la soumission de requêtes par des agents d'autorités chargées de l'application de la loi ou organismes administratifs.

Apple considère qu'une demande d'informations par une autorité chargée de l'application de la loi est juridiquement valide si elle est effectuée dans des circonstances liées de bonne foi à la prévention ou la détection d'infractions ou à des enquêtes sur des infractions, et répondra de façon appropriée à ce qu'elle estime être des requêtes juridiquement valides.

B. Demandes de préservation

Toutes les données iCloud stockées par Apple sont chiffrées à l'emplacement du serveur. Lorsqu'il est fait appel à des revendeurs tiers pour stocker des données, Apple ne leur donne jamais les clés de chiffrement. Apple conserve les clés de chiffrement dans ses centres de données aux États-Unis. Les autorités chargées de l'application de la loi situées en dehors des États-Unis qui cherchent à obtenir ce type de contenu sont tenues de suivre la procédure judiciaire devant les autorités du Ministère de la Justice américain. Si le pays étranger a signé un Traité d'entraide judiciaire mutuelle avec les États-Unis, la procédure judiciaire appropriée sera celle stipulée par les dispositions du traité ou dans le cadre d'autres efforts de collaboration avec les autorités du Ministère de la Justice américain. Si la préservation des données est demandée avant une procédure imminente dans le cadre du Traité d'entraide judiciaire, la requête devra être soumise à Apple Inc. par e-mail à subpoenas@apple.com. Les demandes de préservation doivent comporter l'identifiant Apple/l'adresse e-mail du compte, ou le nom complet et le numéro de téléphone et/ou le nom complet et l'adresse postale du compte Apple en question.

Une fois la demande de préservation reçue, Apple Inc. préservera une seule importation des données existantes de l'utilisateur demandées et disponibles au moment de la demande, pendant une durée de 90 jours. Au-delà de cette période de 90 jours, les données préservées seront automatiquement supprimées du serveur de stockage. Cependant, cette période pourra être prolongée de 90 jours si la demande est renouvelée. Plus de deux demandes de préservation pour un même compte seront traitées comme des demandes d'extension des données préservées initialement, mais Apple Inc. ne procèdera pas à la préservation de nouvelles données en réponse à de telles requêtes.

C. Demandes urgentes

Apple considère une demande comme urgente lorsqu'elle est liée à des circonstances qui, de bonne foi, constituent une menace immédiate et sérieuse :

1) pour la liberté ou la sécurité d'une ou de plusieurs personnes ;
2) pour la sécurité d'un État ;
3) de commettre des dommages substantiels à des infrastructures ou des installations essentielles.

Si l'agent à l'origine de la demande apporte la confirmation satisfaisante que sa requête porte de bonne foi sur une circonstance urgente satisfaisant à un ou plusieurs des critères ci-dessus, Apple l'examinera en urgence.

Pour effectuer une demande urgente auprès d'Apple, l'agent à l'origine de la demande doit remplir le formulaire intitulé « Demande d'informations URGENTE pour une autorité chargée de l'application de la loi » figurant à l'annexe B et le transmettre directement depuis l'adresse e-mail officielle de son service à : exigent@apple.com, avec la mention « Emergency Law Enforcement Information Request» (« Demande d'informations urgente pour une autorité chargée de l'application de la loi ») dans la ligne d'objet.

Si Apple fournit des données sur des clients en réponse à une telle demande, le responsable de l'agent ayant soumis cette demande d'informations urgente sera contacté et invité à confirmer à Apple la légitimité de cette demande d'informations. Apple exige que l'agent ayant soumis la Demande d'informations urgente pour une autorité chargée de l'application de la loi communique les coordonnées de son responsable lors de la soumission de cette demande.

En outre, cet agent doit également contacter le Global Security Operations Centre (GSOC) d'Apple au +1 408-974-2095, lui indiquer qu'il a effectué une demande d'informations urgente pour une autorité chargée de l'application de la loi, fournir de brefs renseignements sur cette requête et demander qu'elle soit portée à l'attention de l'équipe appropriée en tant que demande urgente. Ce numéro est pris en charge dans toutes les langues.

D. Demandes de suppression de comptes

Si une autorité chargée de l'application de la loi demande à Apple de supprimer l'identifiant Apple d'un client, elle sera tenue de fournir à Apple un mandat ou une décision d'un tribunal spécifiant le compte à supprimer et le fondement de la requête.

E. Notification aux utilisateurs

Apple avertit ses clients quand leurs informations à caractère personnel sont recherchées dans le cadre d'une demande d'informations juridiquement valide d'une autorité chargée de l'application de la loi, sauf si elle juge raisonnablement que cette mesure pourrait entraver le cours de la justice ou nuire à l'administration de la justice.

Pour les demandes urgentes, Apple envoie une notification différée, sauf quand elle juge raisonnablement que cette mesure pourrait entraver le cours de la justice ou nuire à l'administration de la justice. Apple délivre les notifications différées de ces demandes après l'expiration de la période de non-divulgation spécifiée dans la décision du tribunal, sauf si elle juge raisonnablement que cette mesure pourrait entraver le cours de la justice ou nuire à l'administration de la justice.

III. Informations disponibles auprès d'Apple

A. Inscription d'appareils

Les clients qui enregistrent un appareil sous une version antérieure à iOS 8 et OS Yosemite 10.10 transmettent à Apple des informations d'inscription de base ou personnelles, y compris leurs nom, adresse postale, adresse e-mail et numéro de téléphone. Apple ne vérifie pas ces informations et elles peuvent donc être erronées ou ne pas correspondre au propriétaire de l'appareil. Nous recevons des informations d'inscription pour les appareils exécutant iOS 8 (ou versions ultérieures) et les Mac sous OS Yosemite 10.10 (ou versions ultérieures), lorsque le client associe son appareil à un identifiant Apple iCloud. Ces informations peuvent être erronées ou ne pas correspondre au propriétaire de l'appareil. Les informations transmises au cours de l'inscription peuvent être mises à disposition sur présentation d'une demande juridiquement valide.

Veuillez noter que les numéros de série des appareils Apple ne contiennent ni la lettre « O », ni la lettre « I », mais qu'Apple utilise les chiffres 0 (zéro) et 1 (un) dans ces numéros de série. Les demandes avec des numéros de série contenant les lettres « O » ou « I » ne donneront aucun résultat.

B. Dossiers du service clientèle

Les contacts que les clients ont eus avec le service clientèle Apple à propos d'un appareil ou d'un service peuvent être obtenus auprès d'Apple. Ces informations peuvent inclure les dossiers sur les interactions avec les clients dans le cadre d'une assistance pour un appareil ou un service Apple particulier. En outre, des données concernant l'appareil, la garantie et les réparations peuvent aussi être mises à disposition. Ces informations peuvent être obtenues sur présentation d'une demande juridiquement valide.

C. iTunes

iTunes est une application logicielle gratuite dont se servent les clients pour organiser et lire de la musique et des vidéos numériques sur leurs ordinateurs. C'est aussi un magasin qui leur propose du contenu à télécharger pour leurs ordinateurs et appareils iOS. Quand des clients créent un compte iTunes, ils peuvent communiquer des informations de base comme leurs nom, adresse postale, adresse e-mail et numéro de téléphone. De plus, des données sur les transactions et connexions liées aux achats/téléchargements sur iTunes, ainsi que les connexions liées à des mises à jour/nouveaux téléchargements et les connexions iTunes Match, peuvent aussi être mises à disposition. Les informations sur les abonnés iTunes et les journaux de leurs connexions avec les adresses IP peuvent être obtenues sur présentation d'une demande juridiquement valide.

Les historiques des transactions liées à des achats/téléchargements sur iTunes sont contrôlés par iTunes S.à.r.l., une société luxembourgeoise. En raison des dispositions législatives, iTunes ne peut répondre aux requêtes de ce type que si elles ont été validées par le Parquet général luxembourgeois puis transmises à iTunes pour obtenir une réponse. Ces demandes doivent être envoyées au Parquet général du Luxembourg à l'adresse suivante : Parquet général, Procureur général d'État, Cité Judiciaire Bât. CR, Plateau du St Esprit, L-2080 LUXEMBOURG, numéro de fax : +352 47 05 50, adresse e-mail : parquet.general@justice.etat.lu.

D. Transactions dans un Apple Store

Les transactions en magasin sont des transactions effectuées en espèces, par carte bancaire ou cartes cadeaux dans un Apple Store. Une demande juridiquement valide est exigée pour obtenir des informations sur le type de carte associé à un achat particulier, le nom de l'acheteur, son adresse e-mail, la date et l'heure de la transaction, son montant et l'adresse du magasin. Lors d'une demande d'informations juridiquement valide portant sur les dossiers d'un magasin, le numéro complet de la carte bancaire utilisée et toute information supplémentaire comme la date et l'heure de la transaction, le montant et les articles achetés doivent être communiqués. En outre, les autorités chargées de l'application de la loi peuvent fournir à Apple le numéro du ticket de caisse associé à l'achat afin d'obtenir des duplicatas de ces tickets de caisse en réponse à une demande juridiquement valide.

E. Achats sur l'Apple Store en ligne

Apple conserve les informations relatives aux achats en ligne, y compris le nom, l'adresse d'expédition, le numéro de téléphone, l'adresse e-mail, le produit acheté, le montant de l'achat et l'adresse IP de l'achat. Une demande juridiquement valide est nécessaire pour obtenir ces informations. Pour les demandes d'informations concernant des commandes en ligne (à l'exclusion des achats sur iTunes), un numéro de carte bancaire complet, un numéro de commande, un numéro de référence ou le numéro de série de l'article acheté est nécessaire. Le nom du client associé à ces paramètres peut être également fourni, mais le nom du client seul ne suffit pas pour obtenir ces informations.

F. Cartes Cadeaux iTunes

Les Cartes Cadeaux iTunes comportent un code alphanumérique à seize chiffres situé sous la partie grise à gratter au dos de la carte et un code à dix-neuf chiffres situé en bas de la carte. À partir de ces codes, Apple peut déterminer si la carte a été activée[1] ou utilisée et si des achats ont été effectués sur le compte associé à la carte. Lorsque les Cartes Cadeaux iTunes sont activées, Apple enregistre le nom et l'adresse du magasin, ainsi que la date et l'heure. Si les Cartes Cadeaux iTunes sont utilisées pour des achats sur l'iTunes Store, elles sont alors associées à un compte utilisateur. Les Cartes Cadeaux iTunes achetées sur l'Apple Store en ligne peuvent être localisées dans les systèmes Apple par leur numéro de commande Apple Store en ligne. (Remarque : ceci s'applique uniquement aux Cartes Cadeaux iTunes achetées auprès d'Apple et non auprès de distributeurs tiers.) Les informations concernant le client ayant utilisé ces cartes ne peuvent être fournies qu'en présence d'une requête juridiquement valide. De plus, pour les informations sur les achats effectués sur l'iTunes Store, la demande doit être adressée au Parquet général luxembourgeois à l'adresse suivante : Parquet général, Procureur général d'État, Cité Judiciaire Bât. CR, Plateau du St Esprit, L-2080 LUXEMBOURG, numéro de fax : +352 47 05 50, adresse e-mail : parquet.general@justice.etat.lu.

Apple ne peut pas désactiver des Cartes Cadeaux iTunes en réponse à une demande juridiquement valide d'une autorité chargée de l'application de la loi ou d'un organisme administratif.

G. iCloud

iCloud est un service d'Apple qui permet aux utilisateurs d'accéder à leur musique, leurs photos, leurs documents et plus encore à partir de tous leurs appareils. Les abonnés peuvent également sauvegarder le contenu de leurs appareils iOS sur iCloud. Avec le service iCloud, ils peuvent créer un compte de messagerie iCloud.com. Les noms de domaine de la messagerie iCloud peuvent être @icloud.com, @me.com[2] et @mac.com. Toutes les données iCloud stockées par Apple sont chiffrées à l'emplacement du serveur. Lorsqu'il est fait appel à des revendeurs tiers pour stocker des données, Apple ne leur donne jamais les clés. Apple conserve les clés de chiffrement dans ses centres de données aux États-Unis.

iCloud est un service par abonnement. Les demandes de données iCloud doivent inclure l'identifiant Apple/l'adresse e-mail du compte. Si l'identifiant Apple ou l'adresse e-mail du compte ne sont pas connus, Apple exige des informations sur l'abonné comme son nom complet **et** son numéro de téléphone et/ou son nom complet **et** son adresse postale afin d'identifier le compte Apple concerné.

---

[1] « Activée » signifie que la carte a été achetée dans un point de vente, mais n'a été ni utilisée ni remboursée.

[2] iCloud a remplacé le service MobileMe. Par conséquent, Apple n'a plus aucun contenu séparé lié aux anciens comptes MobileMe. Si le contenu ne se trouve pas dans iCloud, cela signifie qu'il n'est plus stocké.

Les informations ci-dessous peuvent être mises à disposition à partir d'iCloud :

i. Informations sur l'abonné

Quand un client crée un compte iCloud, des informations de base sur cet abonné comme ses nom, adresse postale, adresse e-mail et numéro de téléphone peuvent être communiquées à Apple. De plus, des données concernant les connexions aux fonctionnalités iCloud peuvent aussi être mises à disposition. Les informations sur les abonnés iCloud et les journaux des connexions avec les adresses IP peuvent être obtenus sur présentation d'une demande juridiquement valide. Les journaux des connexions sont conservés pendant une durée allant jusqu'à 30 jours.

ii. Journaux d'e-mails

Les journaux d'e-mails d'iCloud comprennent des enregistrements de données telles que la date et l'heure des communications entrantes et sortantes, ainsi que les adresses e-mail des expéditeurs et des destinataires. Ces journaux peuvent être obtenus sur présentation d'une demande juridiquement valide. Ils sont conservés pendant une durée allant jusqu'à 60 jours.

iii. Contenu des e-mails et autres contenus iCloud. Sauvegardes des appareils iOS, flux de photos, documents, contacts, calendriers et signets

iCloud stocke uniquement le contenu qu'un abonné a décidé de conserver sur son compte lorsque ce dernier est actif. Le contenu iCloud peut inclure des sauvegardes d'e-mails, de photos stockées, de documents, de contacts, de calendriers, de signets et d'appareils iOS. La sauvegarde d'un appareil iOS peut inclure les photos et vidéos contenues dans la Pellicule de l'utilisateur, les paramètres de l'appareil, les données des apps, les iMessage, les SMS et MMS et les données de messagerie vocale. Toutes les données iCloud stockées par Apple sont chiffrées à l'emplacement du serveur. Lorsqu'il est fait appel à des revendeurs tiers pour stocker des données, Apple ne leur donne jamais les clés. Apple conserve les clés de chiffrement dans ses centres de données aux États-Unis. Les autorités chargées de l'application de la loi situées en dehors des États-Unis qui cherchent à obtenir ce type de contenu sont tenues de suivre la procédure judiciaire devant les autorités du Ministère de la Justice américain. Si le pays étranger a signé un Traité d'entraide judiciaire mutuelle avec les États-Unis, la procédure judiciaire appropriée sera celle stipulée par les dispositions du traité ou dans le cadre d'autres efforts de collaboration avec les autorités du Ministère de la Justice américain. Apple Inc. fournira le contenu de l'abonné, tel qu'il existe sur son compte, uniquement en réponse à un mandat de perquisition émis conformément à la procédure stipulée dans le Traité d'entraide judiciaire mutuelle.

Apple ne conserve pas le contenu supprimé une fois qu'il a été effacé de ses serveurs.

H. Localiser mon iPhone

Localiser mon iPhone est une fonction activée par l'utilisateur qui permet à un abonné iCloud de localiser son iPhone, iPad, iPod touch ou Mac lorsqu'il l'a perdu et/ou de prendre certaines mesures comme mettre l'appareil en mode Perdu, le verrouiller ou en effacer le contenu. Des informations supplémentaires sur ce service sont disponibles à l'adresse http://www.apple.com/befr/icloud/find-my-iphone.html. Les informations sur l'emplacement d'un appareil localisé par la fonction Localiser mon iPhone sont destinées à l'utilisateur et Apple ne dispose pas de dossiers sur les plans ou les alertes par e-mail fournis par le biais de ce service. Des journaux des connexions Localiser mon iPhone peuvent être mis à disposition et obtenus avec une demande juridiquement valide. Ces journaux sont disponibles pendant une période de 30 jours environ. L'activité Localiser mon iPhone liée aux demandes de verrouillage ou

d'effacement à distance d'un appareil peut être mise à disposition uniquement sur présentation d'une demande juridiquement valide.

Apple ne peut activer cette fonction sur l'appareil d'un utilisateur à la demande des autorités chargées de l'application de la loi. La fonction Localiser mon iPhone doit avoir été préalablement activée par l'utilisateur pour cet appareil spécifique. Apple ne dispose pas d'informations GPS pour un appareil ou un utilisateur particulier.

I. Extraction de données d'appareils iOS verrouillés par un code

Les demandes d'assistance technique pour accéder à du contenu sur des appareils spécifiques doivent être adressées à Apple Inc. via la procédure stipulée dans le Traité d'entraide judiciaire mutuelle. Les autorités chargées de l'application de la loi situées en dehors des États-Unis qui cherchent à obtenir ce type de contenu sont tenues de suivre la procédure judiciaire devant les autorités du Ministère de la Justice américain. Si le pays étranger a signé un Traité d'entraide judiciaire mutuelle avec les États-Unis, la procédure judiciaire appropriée sera celle stipulée par les dispositions du traité ou dans le cadre d'autres efforts de collaboration avec les autorités du Ministère de la Justice américain.

Pour tous les appareils sous iOS 8.0 ou versions ultérieures, Apple ne pourra pas procéder à des extractions de données iOS car les outils d'extraction de données sont désormais inopérants. Les fichiers à extraire sont protégés par une clé de chiffrement liée au code confidentiel de l'utilisateur qu'Apple ne possède pas.

Pour les appareils iOS exécutant des versions d'iOS antérieures à iOS 8.0, Apple peut, sur présentation d'un mandat de perquisition émis conformément à la procédure stipulée dans le Traité d'entraide judiciaire mutuelle, extraire certaines catégories de données actives à partir d'appareils iOS verrouillés par un code. Plus précisément, l'utilisateur a généré des fichiers actifs sur un appareil iOS, qui sont contenus dans des apps natives d'Apple et pour lesquels les données ne sont pas chiffrées par le code confidentiel (« fichiers actifs générés par l'utilisateur ») ; ces données peuvent donc être extraites et transmises aux autorités chargées de l'application de la loi sur des supports externes. Apple Inc. peut procéder à une extraction des données sur les appareils iOS exécutant iOS 4 jusqu'à iOS 7. Veuillez noter que les seules catégories de fichiers actifs générés par l'utilisateur susceptibles d'être transmises à une autorité chargée de l'application de la loi, sur présentation à Apple Inc. d'un mandat de perquisition émis conformément à la procédure stipulée dans le Traité d'entraide judiciaire mutuelle, sont les suivantes : SMS, iMessage, MMS, photos, vidéos, contacts, enregistrements audio et historique des appels. Apple Inc. ne peut fournir ce qui suit : e-mails, entrées des calendriers et données d'apps tierces.

L'extraction des données ne peut être réalisée qu'au siège d'Apple Inc. à Cupertino, en Californie, pour des appareils en bon état de marche. Pour qu'Apple Inc. apporte son assistance à la procédure, la formulation désignée ci-dessous doit figurer dans le mandat de perquisition et ce mandat doit comprendre le numéro de série ou le numéro IMEI de l'appareil. Pour de plus amples informations sur l'emplacement d'un numéro de série ou d'un numéro IMEI, consultez : http://support.apple.com/kb/ht4061.

Veuillez vous assurer que le nom du juge figurant sur le mandat de perquisition soit imprimé clairement et lisiblement en vue des formalités administratives.

Une fois que l'autorité chargée de l'application de la loi a obtenu un mandat de perquisition avec la formulation indiquée, elle peut le remettre à Apple Inc. en l'envoyant par e-mail à l'adresse subpoenas@apple.com. Pour l'extraction des données, l'appareil iOS peut être remis à Apple Inc. soit sur rendez-vous soit par courrier. Si l'autorité chargée de l'application de la loi choisit

d'expédier l'appareil, il ne doit pas être envoyé avant que l'agent de l'autorité concernée ne reçoive un e-mail d'Apple qui en demande l'expédition.

Pour l'extraction des données sur rendez-vous, Apple exige que l'agent de l'autorité chargée de l'application de la loi apporte un disque dur FireWire avec une capacité de stockage au minimum égale à deux fois la capacité mémoire de l'appareil iOS. Si l'autorité chargée de l'application de la loi choisit d'expédier l'appareil, elle doit fournir à Apple un disque dur externe ou une clé USB avec une capacité de stockage au minimum égale à deux fois la capacité mémoire de l'appareil iOS. Vous êtes prié de ne pas envoyer l'appareil avant d'avoir reçu un e-mail demandant son expédition.

Une fois l'extraction des données effectuée, une copie du contenu généré par l'utilisateur sur l'appareil vous sera fournie. Apple Inc. ne conserve pas de copies des données de l'utilisateur extraites au cours de la procédure ; de la même manière, la préservation de toutes les preuves relève de la responsabilité de l'autorité chargée de l'application de la loi.

Formulation requise pour le mandat de perquisition :

> « Il est ordonné, par le présent mandat, qu'Apple Inc. aide [AUTORITÉ CHARGÉE DE L'APPLICATION DE LA LOI] dans sa recherche d'un appareil iOS, modèle n° _____, sur le réseau _____ avec le numéro d'accès (numéro de téléphone) _____, le numéro de série[3] ou le numéro IMEI[4] _____ et l'identifiant FCC n° _____ (l'« Appareil »), en lui apportant une assistance technique raisonnable si l'Appareil est en bon état de fonctionnement et a été verrouillé par un code confidentiel. Cette assistance raisonnable consiste, dans la mesure du possible, à extraire les données de l'Appareil, à les copier sur un disque dur externe ou un autre support de stockage et à retourner le support de stockage susmentionné à l'autorité chargée de l'application de la loi. L'autorité chargée de l'application de la loi pourra ensuite effectuer une recherche des données de l'appareil sur le support de stockage fourni.
>
> Il est ordonné également, dans la mesure où les données contenues sur l'Appareil sont chiffrées, qu'Apple fournisse une copie des données chiffrées à l'autorité chargée de l'application de la loi, mais Apple n'est pas tenue d'essayer de déchiffrer les données ou de permettre autrement à cette autorité d'essayer d'y accéder.
>
> Bien qu'Apple fasse tous les efforts raisonnables pour maintenir l'intégrité des données contenues sur l'Appareil, il ne pourra être exigé d'Apple qu'elle conserve des copies des données de l'utilisateur du fait de l'assistance ordonnée par le présent mandat ; la préservation de toutes les preuves relève de la responsabilité de l'autorité chargée de l'application de la loi. »

---

[3] Veuillez noter que les numéros de série des appareils Apple ne contiennent ni la lettre « O », ni la lettre « I », mais qu'Apple utilise les chiffres 0 (zéro) et 1 (un) dans ces numéros. Il n'est donc pas possible de procéder à des extractions de données iOS pour les appareils dont le numéro de série contient les lettres « O » ou « I ».

[4] Le numéro IMEI est gravé au dos des iPad Cellular, de l'iPhone d'origine et des iPhone 5, 5c, 5s, 6 et 6 Plus. Pour de plus amples informations, consultez le site http://support.apple.com/kb/ht4061. Veuillez noter que, pour les modèles ayant un numéro IMEI gravé sur le logement de carte SIM, ce logement dans l'appareil peut ne pas être le logement d'origine livré avec l'appareil.

J. Autres informations disponibles sur l'appareil

Adresse MAC : une adresse MAC (Media Access Control) est un identifiant unique attribué à des interfaces réseau pour les communications sur le segment du réseau physique. Un produit Apple avec des interfaces réseau aura une ou plusieurs adresses MAC, y compris Bluetooth, Ethernet, Wi-Fi ou FireWire. Cette information peut être obtenue avec une demande juridiquement valide en fournissant à Apple un numéro de série (ou dans le cas d'un appareil iOS, un numéro IMEI, MEID ou UDID).

UDID : l'identifiant UDID (unique device identifier) est une séquence de 40 lettres et chiffres qui est spécifique à un appareil iOS particulier. Il se présente comme suit : 2j6f0ec908d137be2e1730235f5664094b831186.

Si l'autorité chargée de l'application de la loi est en possession de l'appareil, il peut être connecté à iTunes pour obtenir l'UDID. L'UDID peut être révélé en cliquant sur le numéro de série de l'appareil sous l'onglet Résumé d'iTunes.

K. Demandes des vidéos de surveillance d'un Apple Store

Les enregistrements des vidéos de surveillance peuvent varier d'un magasin à l'autre. Ils sont conservés par l'Apple Store pendant une durée maximale de trente jours. Dans nombre de pays européens, cette durée peut être limitée à seulement 24 heures en raison des législations locales. Une fois ce délai expiré, la vidéo de surveillance n'est plus disponible. Les demandes de vidéos de surveillance par une autorité chargée de l'application de la loi peuvent être effectuées auprès de n'importe quel Apple Store local. S'agissant de la vidéo demandée, l'autorité chargée de l'application de la loi doit fournir une date et une heure spécifiques et les informations concernant la transaction.

L. Game Center

Game Center est le réseau social de jeux d'Apple. Des informations sur les connexions d'un utilisateur à Game Center peuvent être mises à disposition. Les journaux des connexions avec les adresses IP et l'historique des transactions sont mis à disposition uniquement sur présentation d'une demande juridiquement valide.

M. Activation d'appareils iOS

Quand un client active un appareil iOS ou met à jour le logiciel, certaines informations sont fournies à Apple par le prestataire de services ou à partir de l'appareil, selon l'évènement. Les adresses IP de l'évènement, les numéros ICCID et autres identifiants peuvent être mis à disposition. Ces informations sont mises à disposition uniquement sur présentation d'une demande juridiquement valide.

N. Journaux des connexions

L'activité d'un utilisateur ou d'un appareil liée aux connexions à des services Apple tels qu'iTunes, iCloud, Mon identifiant Apple et Forums Apple, peut être obtenue auprès d'Apple, si elle est disponible. Les journaux des connexions avec les adresses IP et l'historique des transactions sont mis à disposition uniquement sur présentation d'une demande juridiquement valide.

O. Journaux iForgot et Mon identifiant Apple

Les journaux iForgot et Mon identifiant Apple d'un utilisateur peuvent être obtenus auprès d'Apple. Ils peuvent inclure des informations sur les réinitialisations de mot de passe. Les journaux des connexions avec les adresses IP et l'historique des transactions sont mis à disposition uniquement sur présentation d'une demande juridiquement valide.

P. FaceTime

Les communications FaceTime sont chiffrées de bout en bout et Apple n'a aucun moyen de déchiffrer les données FaceTime qui transitent entre les appareils. Apple ne peut intercepter des communications FaceTime. Apple dispose des journaux des invitations à un appel FaceTime lorsqu'elles sont initiées. Ces journaux n'indiquent pas que des communications entre les utilisateurs ont réellement eu lieu. Apple n'a aucune information lui permettant de vérifier qu'un appel FaceTime a été bien établi ou de connaître la durée d'un appel FaceTime. Les journaux des invitations à des appels FaceTime sont conservés pendant une durée allant jusqu'à 30 jours. Ils sont mis à disposition uniquement sur présentation d'une demande juridiquement valide.

IV. Questions et réponses

Q : Puis-je adresser des questions à Apple dans le cadre de ma procédure judiciaire ou de ma demande d'informations en tant qu'autorité chargée de l'application de la loi ?
R : Oui. Les questions ou requêtes dans le cadre de votre demande d'informations doivent être adressées à law.enf.emeia@apple.com.

Q : Un appareil doit-il être inscrit auprès d'Apple pour fonctionner ou être utilisé ?
R : Non. Un appareil ne doit pas être obligatoirement inscrit auprès d'Apple pour fonctionner ou être utilisé.

Q : Apple peut-elle me transmettre le code d'un appareil iOS actuellement verrouillé ?
R : Non. Apple n'a pas accès au code confidentiel de l'utilisateur. Mais, selon la version d'iOS sous laquelle l'appareil fonctionne, Apple peut être en mesure d'extraire certaines données d'un appareil verrouillé, sur présentation d'un mandat de perquisition valide émis conformément à la procédure stipulée dans le Traité d'entraide judiciaire mutuelle, comme il est indiqué dans ces recommandations.

Q : Apple stocke-t-elle des informations GPS susceptibles d'être communiquées dans le cadre d'une demande juridiquement valide ?
R : Non. Apple ne suit pas la géolocalisation des appareils.

Q : Que convient-il de faire avec les informations fournies en réponse, lorsque l'autorité chargée de l'application de la loi a conclu l'enquête/l'affaire pénale ?
R : Apple exige que toutes les informations et données contenant des informations personnellement identifiables (y compris toutes les copies effectuées), transmises à une autorité chargée de l'application de la loi, soient détruites après que l'enquête ou l'affaire pénale liée est conclue et que tous les appels sont épuisés.

Q : Informez-vous les utilisateurs concernés par des demandes d'informations des autorités chargées de l'application de la loi ?
R : Oui. Apple avertit les clients concernés quand les informations à caractère personnel de leur compte sont recherchées dans le cadre d'une demande d'informations juridiquement valide d'une autorité chargée de l'application de la loi, sauf si elle juge raisonnablement que cette mesure pourrait entraver le cours de la justice ou nuire à l'administration de la justice.

Q : Pouvez-vous m'aider à restituer un appareil perdu ou volé à son propriétaire légitime ?
R : Si vous, en tant qu'autorité chargée de l'application de la loi dans la région EMEIA, avez récupéré un appareil soupçonné d'avoir été perdu ou volé et souhaitez le restituer à son « propriétaire légitime », vous devez envoyer votre demande à l'adresse law.enf.emeia@apple.com et inclure le numéro de série ou IMEI de l'appareil et toutes les informations supplémentaires utiles. Si des informations sur l'inscription de l'appareil sont disponibles, nous contacterons la personne inscrite et nous lui conseillerons de s'adresser à vous.

V. Annexe A

Le formulaire Demande d'informations pour une autorité chargée de l'application de la loi pour la région géographique EMEIA est disponible sous forme de PDF éditable à l'adresse : http://www.apple.com/legal/privacy/emeia-le-inforequest.pdf

VI. Annexe B

Le formulaire Demande d'informations URGENTE pour une autorité chargée de l'application de la loi pour la région géographique EMEIA est disponible sous forme de PDF éditable à l'adresse : http://www.apple.com/legal/privacy/le-emergencyrequest.pdf