参考資料1

第13回会合における事業者からの主な発言（追加）

2022年6月27日

事　　務　　局

事業者への質疑応答①

プライバシーに関して非常に積極的に取り組んでおり、業界を主導しているところと認識。業界の動きもあり、ユーザーがどういうことを望んでいるのかが重要になるので、原則の中に、ユーザーとの対話を４原則の５番目として入れていただけないか。【佐藤構成員】

Apple Inc.

- プライバシーに対する積極的な取り組みは、競争上の差別要因と考えている。
- 私たちが行う全てのことについて、ユーザーとの対話は不可欠であり、根幹を成すものと考えている。
- 当社の原則の3つ目にある「透明性とコントロール」は、自身のデータがどのように収集されて処理されるのかをユーザーがしっかりと理解し、それを踏まえてユーザーが選択できることを確かなことにすべく、正面から取り組むものである。加えて、プライバシーポリシーの中に、ユーザーから直接問い合わせを書いて送っていただく、あるいは質問いただく方法が用意されており、アイルランドのコーク市にあるチームが多言語対応をしている。他の大規模プラットフォームとの違いとして、顧客を一人と捉えている点がある。当社のデバイスを持っているユーザーが唯一の顧客と考えている。

Apple Payで物を買ったときに店の情報として位置情報が取れたり、といったように、間接的にいろいろな方法で位置情報が取れる。そういった間接的に取得する位置情報に関しては、どのような取組をされているか。【佐藤構成員】

Apple Inc.

- Apple Payを使っても、そういった顧客の情報は把握しないことになっている。位置情報データは、ユーザーが位置情報サービスを有効にしている場合にのみ送信される可能性があり、匿名で送信される。

事業者への質疑応答②

モニタリングシート1.4のApp Storeについて、App StoreでAppleが収集したデータと、Safari経由でAppleが収集したデータを組み合わせて（複数のレイヤーをまたいでデータを組み合わせて）、Appleが分析・利用する場合はあるのか。【小林構成員】

Apple Inc.

■ Safariそのものがごくわずかなデータしか収集しない。プライバシーありきで最初から設計されているのでそのようになっており、Safariのデータ とApp Storeのデータは統合されない。

App Storeで収集したデータはAppleの広告プラットフォームに保存されると、そのデータを製品開発や他のサービス開発などに自社内で利用することはあるのか。Appleは非常に大きなプラットフォーム事業者なので、レイヤー間でサービス間でデータを共有するということも、他社と共有するくらいのプライバシーインパクトがあり得るのではないか。【小林構成員】

Apple Inc.

■ App Storeはごくわずかなデータしか収集せず、競争的な製品開発をする上で使用していない。当社のデータ収集で製品サービスに活用されるものはデータの最小化を行っているので、App Storeで収集されるデータは、サービス提供はもとより必要な範囲に限られる。あくまでもApp Storeのサービスを提供する上で必要なデータしか収集していない。Appleの広告による収集においては、自社ファーストパーティデータのみを使用している。

モニタリングシートの2.12のデータポータビリティについて、ユーザーがダウンロードするところまでが書かれているが、他のプラットフォームにそのまま移転できるようなサービスについては、どこまで検討が進んでいるか。【小林構成員】

Apple Inc.

■ DTPの一員として資金も拠出し、他社との協力関係を積極的に進めている。ポータビリティに加え、インターオペラビリティにも取り組んでおり、作業が円滑に進んでいると聞いている。多岐にわたるプラットフォーム間でのインターオペラビリティは、それなりの困難が伴う。

事業者への質疑応答③

ユーザーのプライバシーへの取り組みは大変立派なものだと考えており、ありがたい。サイドローディングを認めることを義務化する政策提案が日本でなされているが。この提案についてどのように考えるか。【森構成員】

Apple Inc.

- プライバシーとセキュリティの観点から簡潔に申し上げると、ユーザーは損害を被ることになる。Apple Storeのメリットがサイドローディングによって損なわれるからである。
- App Tracking Transparency (ATT)は単なる技術ではなく理念でもある。トラッキングを防止する上で、ATTを使って追跡を拒否すると、OSはアプリに対して、IDFAを利用することを制限し、技術的に阻止するだけでなく、アプリに対して他の方法を使ってもトラックしないようにシグナルを送ることになる。アプリ審査の一部としてアプリを提出するプロセスにおいて、アプリが実際にそのユーザーに追跡されることを許可しないとすると、本当に追跡しないかどうかの確認をつぶさに行っている。（ユーザーの許可なしに）ユーザー情報を追跡したいアプリはApp Storeにのせられないこととなっているが、サイドローディングを許可すれば、それができてしまうことになる。
- Androidではサイドローディングが可能だが、iOSに比べるとAndroidの方がマルウェアの数が98%も多いことがわかっている。iOSを乱用するための手段をダークウェブで探そうとすると、かなり手に入りにくいので数億ドルという金額がつく。他方、Androidを乱用するための手段は、サイドローディングすればいいので、かなり安価に入手可能。カナダは濃厚接触者の追跡アプリをApp StoreとGoogle Play両方で提供したが、ハッカーが見た目そっくりのアプリを作ってAndroid上でサイドローディングによって提供してしまった。それが実際にはランサムウェアのアプリだったことが判明している。
- App Storeの場合、どのデベロッパであってもアプリをのせたい場合には必ず本人の名前で登録し、厳格なアプリの審査を経る必要があり、プライバシーとセキュリティの観点からみると、App Storeの方がはるかに優れた機能を有している。
- ソフトウェアエンジニアリングの責任者がよく言っているが、iPhoneを開発する際に、Macでの学びを全て活用してセキュリティとプライバシー保護を強化したとのこと。

事業者への質疑応答④

Apple Inc.のプライバシー保護は、AppStoreがOSと一体であることを前提にしていると思うが、欧州・日本の当局がサイドローディング（野良ストアの開放）を求めている状況にあると思う。野良ストアが開放された場合、現在のプライバシー・セキュリティは確保できるのか。【板倉構成員】

Apple Inc.

■ シンプルな回答は「ノー」になる。サイドローディングに関する規制要求が実現することには強い懸念を抱いている。サイドローディングを防ぐという決定は、App Storeを立ち上げる前になされたもので、iPhoneを安全で、堅牢で、信頼性が高く、使いやすいものにするというAppleの目標に沿って行われたものであった。

■ 仮にAppleが別のアプリストアやサイドローディングを認めるように強制されたなら、マルウェアによる攻撃リスクの増加により、すべてのユーザーがより大きな危険にさらされてしまうだろう。App Storeは現在行われている攻撃を検知し、ブロックするように作られているが、脅威モデルが変化すれば、より高度な攻撃に対するこのような保護機能はすり抜けられてしまう。そうなれば詐欺師たちは新たに開発したツールとノウハウを使って第三者ストアやApp Storeを標的にするため、App Storeだけでアプリをダウンロードする人も含めて、全てのユーザーをより大きな危険にさらすことになる。しかも、マルウェアはエントリポイントとなるアプリに影響するだけでは収まらないだろう。例えば、過度なバッテリーの消耗や侵略的なデータ収集などの影響がダウンロード済みのアプリを妨害するため、他のアプリの機能を深刻に低下させることが起こり得る。潜在的な危険性としてさらに深刻なことに、あるデバイスに侵入したマルウェアは、そのデバイスが接続される別のデバイスやシステムへのアクセスを可能にするための足がかりとして使用され得る。個々のモバイルデバイスは、エンタープライズ環境でネットワーク規模の攻撃を拡散するための共通のエントリポイントとして認識されている。さらに、ユーザーのデバイスから取得した個人情報にアクセスできることで、攻撃者は、ユーザーの友人や家族に対する攻撃を開始するための絶好の立ち位置にいることになる。

事業者への質疑応答⑤

Apple Inc.

（つづき）

■　加えて、不正なアプリのリスクの増加により、ユーザーだけでなく、デベロッパもより大きなリスクにさらされるだろう。日本の情報推進機構（IPA）によれば、消費者から相談を受けたケースの中で、iOSでのマルウェア感染が非常に稀であるだけでなく、違法または不正なアプリに関連するケースの件数も比較的少ないとのことである。仮にAppleが別のアプリストアやサイドローディングを認めるように強制されるなら、著作権を侵害しているアプリや、違法または不正なアプリが入手しやすくなる可能性が激増することが大いに考えられる。また、子どもに有害になる可能性のあるコンテンツや機能を含むアプリの数も増加するだろう。実際、Appleが提供するペアレンタルコントロールソリューションの「スクリーンタイム」は、サイドローディングされたアプリには機能せず、保護者や子どもたちをサポートするための現行の取り組みも損なわれてしまう。

■　詳しくは次のホワイトペーパー参照（Building a Trusted Ecosystem for Millions of Apps - The important role of App Store protections（数百万のアプリのために信頼できるエコシステムを築く – App Storeの保護が果たす重要な役割）（https://www.apple.com/jp/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_J.pdf））。

Apple Inc.が管理する領域は高いレベルでプライバシーが保護されていることがよく分かった。それ以外の領域は必ずしもそうではないため、世界中でさまざまに規制が検討（もしくは既に実装）されていると理解しているが、どのような規制形態・内容であれば効果的で、かつApple Inc.にとっても受け入れ可能か。【沢田構成員】

Apple Inc.

■　アカウンタビリティは、日本も含めて世界中で、プライバシー規制の重要な柱の1つである。Appleは関連法を順守する責任を果たす。

事業者への質疑応答⑥

透明性を重視するという原則にもかかわらず、なぜ、説明資料は非公開なのか。Apple Inc.は、世の中にある情報を収集する方法や技術を最もよく把握していると思うため、むしろ問題を公開し、Apple Inc.1社だけでなく関係者全体で対策を考えるような方向性は考えていないのか。【寺田構成員】

Apple Inc.

■ プライバシーに関する状況は進化することから、最新の情報を総合的に把握するために、当社は常にユーザーに最新のプライバシーポリシーと説明資料を当社のウェブサイト（https://www.apple.com/jp/privacy/）で確認するように勧めている。

モニタリングシート1.5において、セグメントの最少人数が「5000人」と記載されているが、5000人の根拠は何か。質問意図としては、FLoCの取組はキャンセルとなったものの、今後のターゲティング広告において、セグメントの粒度やユーザー制御が重要な課題になると予想しているからである。【佐藤構成員】

Apple Inc.

■ 目標は、セグメントを再特定できないことを確実にすることである。

Safariでは、ITPによってウェブサイト間のトラッキングを制限しており、そのトラッキングについて、ユーザーの同意を求める機会すら提供されていない。その一方で、アプリではユーザーが同意をすれば、アプリ間のトラッキングが可能になるIDFAを利用することができる。今後の方向性としては、Safariに対してIDFAのような識別子を実装してユーザーの同意により利用できるようにする方向性なのか、アプリにおいてもIDFAを廃止し、一切アプリ間のトラッキングをできないようにしていく方向性なのか、どちらの方向性なのか教えてほしい。【太田構成員】

Apple Inc.

■ 今後の製品やサービスについてのコメントは控えるが、ユーザーに最高のプライバシー保護を提供することに引き続き注力していく。

事業者への質疑応答⑦

AppStoreのプライバシーラベルについて、開発者の自己申告になっており、3rd Party SDKなどの動きを把握できておらず、ラベルの内容と実際のデータ取り扱い状況が食い違っている状況が発生してしまっている認識だが、どのように対応していく計画か。また、Androidが計画しているように、3rd Party SDKについても、AppStoreに登録させるなどの計画はあるか。【太田構成員】

Apple Inc.

■ ユーザーに最高のプライバシー保護を提供するために、常にサービスの反復検証と改善を行っていく。

Private RelayはIngress ProxyとEgress Proxyを分けることによって、Apple Inc.も通信データを見ることはできない仕組みと説明されている。しかし、Ingress ProxyとEgress Proxyが結託することによって通信データを見ることができると思われる。これらが結託しないという保証はどのように実現されているのか。【太田構成員】

Apple Inc.

■ そうした結託を避けるため、当社では次の仕組みを導入している。

■ Private Relayは、ログ記録を最小限にするポリシーにより、ユーザーのIPアドレスやアカウント情報とブラウジング行動を結びつけるのに充分な情報がプロキシのログに含まれないことを確実にするよう設計されている。Private Relayによって記録された情報は、一意の識別子を一切含まず、以下の項目に限られており、サービスの運用および改善のみを目的としている。

- 接続プロパティとパフォーマンス指標
- IPアドレスから取得したネットワークや地域に関する情報
- 匿名トークンの検証の成功率およびパフォーマンス
- Private Relayのシステムリソースの使用量

■ Private Relayの不正防止及び不正対策の一部として、匿名トークンの発行に関連する以下のフィールドがログ記録されるが、接続情報と相互に関連付けることはできない：iCloudアカウント、ソフトウェアのバージョン、リクエストのタイムスタンプ（iCloud Private Relay Overview（iCloud Private Relayの概要）、9ページ「Logging」（ログ記録）を参照。https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF）

事業者への質疑応答⑧

ユーザーへの各種通知について、ユーザーが理解して同意するのが難しいことも多い中、理解を促進するための工夫をしているか。そのための仕組みはあるか。【古谷構成員】

Apple Inc.

■　例えば、AppleのPrivacy Nutrition Labelsを見ると、Apple製アプリを含むそれぞれのアプリがユーザーのデータをどう扱うかがわかるようになっている。（https://www.apple.com/jp/privacy/labels/）。こうした方法で、ユーザーに最高のプライバシー保護を提供するために、常にサービスの反復検証と改善を行っていく。

データミニマイゼーションが達成されている根拠を教えていただきたい。【高橋構成員】

Apple Inc.

■　個人情報を収集しようとする、または収集する全ての製品とサービスは、プライバシー審査を受け、データの最小化の原則が適用される。

入れ替わるランダムな識別子がプライバシーを保護する根拠を教えていただきたい。【高橋構成員】

Apple Inc.

■　デバイスによって生成されるランダムな識別子は、Appleのサーバ上で識別子の役割を果たす。ランダムな識別子が使用されているため、Appleがユーザーを再特定することは不可能。Appleマップの場合だと、セッションごとに（およびセッション自体の間の比較的長いセッションに対して）、Appleマップは新しいランダムな識別子を生成する。

事業者への質疑応答⑨

グリッドスクエアがプライバシーを保護する根拠を教えていただきたい。【高橋構成員】

Apple Inc.

■　こうしたデータのプライバシーを保護するために、当社では世界をグリッドに分割して、それぞれのマスがある種類の検索の1,000回分を表すようにしている。そして、どのグリッドのマスが検索の起点になったのかだけを格納する。そうすることによって常に他の検索が同じマスにあるので、個人の行動が特定の場所に関連付けられないことになる。そして、グリッドのマスを任意のサイズではなく、検索回数を基準にして決めることの優れた点は、常に匿名性が守られることにある。自宅が周囲に何もない場所にあったとしてもである。グリッドのマスを大きくするだけで済む。

App Storeについて、セキュリティ・プライバシーに貢献しているということがよく分かったが、その基準の妥当性に関する専門家によるレビューがあれば教えていただきたい。【高橋構成員】

Apple Inc.

■　参考に次のリンクを御覧いただきたい（https://assets.website-files.com/62715f02a51b614ce64867fd/628e6ba29361afc22807be6b_mobile-future-pathways-to-continued-improvement-in-mobile-security-and-privacy.pdf）。

事業者への質疑応答⑩

Appleはデバイスベンダーでもあるが、iPhoneを含めて、各種デバイスを他のデバイス（他のスマホやパソコン）に直接接続して、バックアップを含めて情報を交換することがある。デバイス間情報交換で、バックアップとそれ以外のケースに分けて、どのようなパーソナルデータがやりとりされるのか。

意図：例えばバックアップ以外のケースで、スマホが取得した行動履歴のうち、パソコンが収集している情報はあるのか（あればその情報）、そしてその情報をどのように使っているのかなどを御説明いただきたい。【佐藤構成員】

Apple Inc.

■ 「デバイス間情報交換」という言葉や、承諾するユーザーに対する透明性がない状態で、パーソナルデータがそうした方法で交換されることについて当社では承知していない。既に述べたように、Appleが、第三者自身のマーケティングのために第三者とパーソナルデータを共有することはない。.