July 3, 2018

Senator Charles E. Grassley
United States Senate
Washington, D.C. 20510

Dear Senator Grassley,

Thank you for your letter regarding the recent events surrounding Facebook and Cambridge Analytica, as well as our data security practices concerning third party developers. We appreciate the opportunity to provide information about our privacy policies and procedures applicable to developers whose apps are made available through the App Store. At Apple, we believe privacy is a fundamental human right, and we design our products to enable and empower users to choose what they share, and with whom. Consistent with this view, we also impose significant restrictions on the apps that may be made available through the App Store. We describe these restrictions, and our applicable policies, further below.

A few significant points, however, are worth mentioning at the outset.

To begin, although your letter refers to "significant concerns regarding the data security practices of large social media platforms," Apple does not provide a social media platform to the public. Rather, to the extent your questions concern the App Store, we highlight that the App Store's primary purpose is to facilitate the distribution of third party software. Although certain apps marketed on the App Store may be social media platforms, or focus on communication or the sharing of information, the App Store itself contains no user generated content outside of app reviews and ratings. Rather, the purpose of the App Store is to provide the best third party apps to Apple's customers. This is in contrast to a social media platform's business model, which depends on providing opportunities for users to share extensive data, which the platform may use to provide services (including advertising) for third party companies.

Given the App Store's role as a marketplace for third party apps, when a customer chooses to download an app to an Apple device, the customer and app developer enter into a direct contractual relationship with one another, governed by the terms of the developer's end user license agreement and privacy policy.

Apple is not a party to these relationships; rather, developers are fully responsible for the content and services they provide in their apps. Notwithstanding the developer's responsibilities and direct relationship with customers, Apple proactively addresses data use issues through its iOS operating system software, and its contract with developers. Apple's iOS operating system software

Apple
One Apple Park Way
Cupertino, CA 95014

T 408 996-1010
F 408 996-0275
www.apple.com

prevents apps from accessing user data stored on the device, such as contacts, calendars, photos, the camera or microphone, location data, health etc. without asking for and obtaining the user's explicit permission. This means that Apple does not decide what user data an app can access, the user does. In addition, Apple sets certain baseline expectations for privacy and data use in its contract with developers, and in its platform guidelines document. App developers must meet these expectations before they can market an app on the App Store and provide users with their own disclosures and choices. These extensive and detailed requirements—which cover a broad range of privacy issues, from data use, to notice, to appropriate consents—reflect our core belief that customers should be in the driver's seat when it comes to choosing what they share, and with whom. We describe these controls in more detail below.

Privacy and Security on the App Store

Apple builds its products and services with user privacy in mind, and the App Store is no exception. Apple's primary business model involves selling, renting, or licensing hardware, software, songs, movies, TV shows, apps, and other services. In brief, these are our products. The customer (and his or her data) is not our product. Apple does not sell or license our customers' personal data to third parties, and we do not otherwise share it with third parties unless our customers direct us to do so, or where such a third party is providing a service to us and is obligated under contract to protect such personal data and use it only as directed by Apple. When Apple collects data (for billing, technical, and service-related or other disclosed purposes) from users who purchase and download apps from the App Store (or our other services), we follow our privacy principles and applicable user agreements.

We protect user data using methods such as encryption, pseudonymization, and aggregation. We believe in providing transparency and control to our users when we collect data. Furthermore, we do not provide data about our customers' actions within third party developer apps unless the user provides an opt-in consent via our analytics program and even that data is collected in a manner that does not identify individual users or devices. We discuss these practices in detail at http://apple.com/privacy.

Privacy Requirements for App Developers

Third party developers that use Apple software to develop apps for the App Store are bound by our Apple Developer Program License Agreement (or PLA). The PLA requires developers to follow rigorous privacy principles. For example, the PLA provides that every app on the App Store must provide clear and complete information to users regarding its collection, use and disclosure of user data and must have a privacy statement or privacy policy if it collects any user data. Apps must also adhere to the App Store Review Guidelines, which expand upon the PLA's requirements on customer privacy. The Guidelines specify, for instance, that apps must include an easily acces-

sible and understandable way for customers to withdraw their consent for any data collected by an app, and apps that violate these rules may be removed from the App Store. Apple also provides developers with access to business management tools that Apple designs with protection of user privacy in mind. In particular, the app analytics we provide allow developers to understand aggregate behavior within their apps without identifying individual users, and only where such users have opted-in to sharing usage data. The privacy requirements placed on third party developers and support provided to them are discussed in more detail below.

iOS Protections for User Data

In addition to the privacy requirements Apple imposes on app developers by contract, Apple's iOS operating system software itself prevents apps from accessing user data without consent. This means that apps cannot access user data, such as contacts, calendars, photos, the camera or microphone, location data, health, etc. without asking for and obtaining the user's explicit permission. iOS also gives customers control over their data by providing them with the ability to withdraw consent later. Through the PLA and Guidelines described above, Apple also requires apps to tell customers about the purpose of the data collection, and to request access only to data that is relevant to an app's core functionality. When a user decides not to grant access to user data (like contacts or location data), we encourage developers to provide alternative solutions, such as allowing a user to manually enter a phone number or physical address.

App Review Process

Before apps can be offered on the App Store, our App Review team of specialists reviews them for compliance with the App Store Review Guidelines, which include rules concerning objectionable content, business model transparency, malware, as well as user privacy. Apps are assigned to specialists trained in the skills required to analyze those apps, and specialists will reject apps they find to be non-compliant with the Guidelines. Specialists then draft a response to the developer explaining the issue and how to resolve it. Developers can then revise the app to bring it into compliance with the Guidelines and resubmit the app for review. During the App Review process, reviewers can escalate potential rule violations for an enhanced review to uncover violations that might not be clear from a typical review. Reviewers also have access to software tools that identify certain processes and methods that are known to violate the Guidelines. Apple works continually to improve its tools, and modify its Guidelines, to address new issues and types of violations. Moreover, our commitment to safety, security, and privacy does not end once apps are on the App Store. New versions of apps must again pass through the App Review process. Furthermore, if we subsequently learn that an app violates either the PLA or the Guidelines, we will investigate to the extent possible, and take appropriate action, as further detailed below.

1. What are your current policies and procedures with respect to sharing of data with third party developers, including how you notify users of such sharing and/or request their consent?

As described above, the App Store is a distribution platform for third party apps. Given the App Store's role as a marketplace for third party apps, when a customer chooses to download an app to an Apple device, the customer and app developer enter into a direct contractual relationship with one another governed by the terms of the developer's end user license agreement and privacy policy. Apple is not a party to these agreements; rather, developers are responsible for the content and services provided in their apps. This means that it is the developer's obligation to collect and use data responsibly and legally.

Apple limits developers' ability to access user data by imposing technical barriers to data collection in its software. In particular, Apple's iOS operating system software prevents apps from accessing user data stored on the device, such as contacts, calendars, photos, the camera or microphone, location data, health, etc. without asking for and obtaining the user's explicit permission. Apple also requires apps to tell the customer about the purpose of the data collection. Apple also includes user controls in Settings that allow users to withdraw consent to share data with a particular app at any time. (Likewise, only if customers consent will Apple provide developers with non-personally identifiable data about how customers use their apps through the App Analytics software tool.)

Apple further seeks to proactively address data use issues through its contractual relationships with developers and its App Review process. And while Apple does not and cannot monitor what developers do with the customer data they have collected or prevent the onward transfer of such data, if Apple obtains credible information that a developer is not acting in accordance with the PLA or Guidelines, Apple will investigate to the extent possible, and take appropriate action, which may include removal of the app from the App Store and removal of the developer from the Apple Developer Program.

Apple enforces its rules and policies for third party apps through the App Review process, in which all apps are reviewed by specialists for their compliance with the Guidelines before they are marketed through the App Store. Apps are assigned to specialists trained in the skills required to analyze those apps, and specialists will reject apps they find to be not in compliance with the Guidelines and draft a response to the developer explaining the issue and how to resolve it. Developers can then revise the app to bring it into compliance with the Guidelines and resubmit the app for review. The App Review team reviews more than 100,000 submissions per week, and rejects approximately 36,000 of those submissions initially due to various Guidelines compliance issues.

Apple's approach to developer privacy practices is not limited to creating and enforcing these rules. We also provide tools and educational materials to encourage developers to design their apps with privacy in mind. Apple's privacy engineers have, for instance, given presentations on topics ranging from differential privacy to data minimization at Apple's annual Worldwide Developer Conference.

a. How have these policies and procedures evolved/changed since 2010?

Apple launched the App Store in 2008 and designed it with user privacy in mind. We have not wavered from that position.

Apple continually evaluates its technical and contractual controls relating to developer access to user data and refines its approach as appropriate. Developers look to collect and use data for evolving purposes, and Apple must learn and adapt as well in order to ensure that its customers' privacy is protected. To that end, we periodically update the PLA and Guidelines to address new privacy issues, such as the introduction of new APIs around health-related human subject research or COPPA compliance. In addition, our App Review team members have access to an ever-evolving set of software tools that identify certain processes and methods that are known to violate the Guidelines.

We have also improved our operating system over time to provide new technical protections for user data with which developers must comply. For example, across multiple releases of our operating systems, we have created "just in time" notices, enforced via operating system security mechanisms, to require users to agree before an app can access certain user data, such as contacts, calendars, photos, the camera or microphone, location data, health, etc. We also started to require apps to include a purpose for the collection of user data to be displayed when the app is requesting access to user data. We have changed location-access prompts—which require users to make an affirmative choice to share their location data—both to offer access only while the application is in use, or access even when the application is not visible. Users are free not to agree to provide developers with the data requested by the developer, and users can revisit their decisions at any time in their device Settings.

b. Do you intend to make any changes in light of recent events?

As described above, we routinely evaluate our policies, procedures, and technical controls and seek to improve upon them, particularly in light of new technology and capabilities.

2. How do you ensure that user data shared with third party developers is not improperly transferred or used?

As an initial matter, it is important to clarify that users, not Apple, determine what personal information to share with apps they choose to download.

In addition, as explained further above, Apple seeks to proactively address data use issues through its contractual relationships with developers and its App Review process. Apple does not and cannot monitor what developers do with the customer data they have collected, or prevent the onward transfer of that data, nor do we have the ability to ensure a developer's compliance with their own privacy policies or local law. The relationship between the app developer and the user is direct, and it is the developer's obligation to collect and use data responsibly, legally, and in accordance with the PLA and Guidelines. However, when we have credible information that a developer is not acting in accordance with the PLA or Guidelines or otherwise violates privacy laws, we will investigate the extent possible, and take appropriate action, which may include removal of the app from the App Store and removal of the developer from the Apple Developer Program. Under the PLA, Apple has the right to terminate a developer's account immediately upon notice for unlawful behavior, which includes privacy violations and misuse of customer data.

3. Do you limit the ability of third party developers to collect data beyond the scope of their application? If so, how do you ensure that third party developer agreements are limited in scope?

iOS has been a leading operating system for isolating users' data in one application from other applications, as well as protecting user data from unwanted access by any application. Apple employs industry leading security and privacy design techniques to "sandbox"—or isolate—applications within containers that hold only data that the application itself generates. Applications are required, by policy and by technical barriers, to receive user consent before accessing user data such as contacts, calendars, photos, the camera or microphone, location data, health, etc.

In addition, the PLA specifically provides that apps must comply with all applicable legal restrictions. Section 3.3.9 states:

> You and Your Applications (and any third party with whom You have contracted to serve advertising) may not collect user or device data without prior user consent, whether such data is obtained directly from the user or through the use of the Apple Software, Apple Services, or Apple SDKs, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising in accordance with **Sections 3.3.12 and 3.3.13**. You may not broaden or otherwise change the scope of usage for previously collected user or device data without obtaining prior user consent for such expanded or

otherwise changed data collection. You may not use analytics software in Your Application to collect and send device data to a third party. Further, neither You nor Your Application will use any permanent, device-based identifier, or any data derived therefrom, for purposes of uniquely identifying a device.

4. What remedies do you have against a third party developer who exceeds the scope of their access?

Developers who do not comply with their privacy obligations under the PLA and/or Guidelines may face one of several repercussions from Apple. For example, if Apple finds an app that is out of compliance with the PLA or Guidelines, Apple may remove the app from the App Store. Apple may also remove the developer from the Apple Developer Program entirely.

5. Do you have protocols built into your third party developer platform to monitor data usage or access?

To protect user privacy, Apple does not track users' activities within an app in a personally identifiable way. And, as described above, Apple does not and cannot, monitor developers' handling of data on their own servers or prevent the onward transfer of data stored on those servers.

Our App Review process provides a means for us to assess app practices over the app lifecycle, as apps are reviewed not only when they are first offered through the App Store but also before any update may be added. When analyzing apps, App Review may use protocols and tools that help it check for unnecessary requests to access data. Furthermore, once App Review is aware of activity or software that might violate the rules set forth in the Guidelines and PLA, App Review can modify its tools to detect such activity or software and reject or escalate apps integrating such software for further review.

6. What audit procedures do you have to ensure compliance with third party developer agreements?

Apple requires that every app, including any new version of an app, pass the App Review process. This process is described further in the response to Question 1.

a. How often have these audits been carried out?

Apple requires developers to submit every new version of their app to App Review before it can be made available to customers on the App Store.

b. How compliant have third party developers been?

Apps are rejected for a large number of reasons. The App Review team reviews more than 100,000 submissions per week, and rejects approximately 36,000 of those submissions initially due to various Guidelines compliance issues. Critically, apps (including updates to apps) cannot be made available on the App Store unless and until they pass App Review.

7. Have third party developers breached your terms/agreements in the past, and what remedies have you taken?

Developers do violate the PLA and Guidelines, although most breaches are unintentional and easily corrected. For example, developers often fail to provide sample login credentials for specialists, or submit an incomplete app for review. In some cases, developers have been known to breach these agreements intentionally and surreptitiously, by deliberately obscuring their bad behavior from our tools. For example, developers may attempt to submit multiple, nearly identical apps in an attempt to "spam" the App Store. Developers engaging in these actions face stiffer penalties.

The most basic penalty is to reject an app or update during the App Review process. If a live app is found to be out of compliance with the PLA and/or the Guidelines, it may be removed from sale from the App Store either permanently or until the issue is resolved.

8. What are your current policies and procedures with respect to notifying users of a data breach?

Apple notifies users of a data breach in accordance with applicable law if and when user information is compromised at Apple or its service providers. Apple does not license or share with developers personally identifiable information that is the subject of data breach laws. Rather, app developers obtain users' information directly from the users with the users' consent; accordingly, developers are responsible for notifying users in accordance with the developers' own legal responsibilities.

a. How have these policies and procedures evolved/changed since 2010?

Apple's data breach notification policy has evolved along with federal, state and international laws since 2010. But fundamentally, our policy is simply to comply with applicable law with respect to the type of data in question as prescribed by the relevant jurisdiction.

b. Do you intend to make any changes in light of recent events?

Apple continually reviews its data incident policy to take account of updates in relevant laws and best practices.

9. What are your current policies and procedures with respect to notifying users of an improper transfer of their data?

Apple notifies users of a data breach in accordance with applicable law if and when user information is compromised at Apple or its service providers. Apple does not license or share with developers personally identifiable information that is the subject of data breach laws. Rather, app developers obtain users' information directly from the users with the users' consent; accordingly, developers are responsible for notifying users in accordance with the developers' own legal responsibilities.

a. How have these policies and procedures evolved/changed since 2010?

Apple's data breach notification policy has evolved along with federal, state and international laws since 2010. But fundamentally, our policy is simply to comply with applicable law with respect to the type of data in question as prescribed by the relevant jurisdiction.

b. Do you intend to make any changes in light of recent events?

Apple continually reviews its data incident policy to take account of updates in relevant laws and best practices.

10. Do you restrict the ability of third party developers to access data for a political purpose?

Apple does not specifically restrict the ability of third party developers to access data for a political purpose. Developers must follow Apple's rules on data collection as set forth in the PLA and Guidelines. As set forth in response to Question 1, developers may only collect data with the user's consent and in accordance with the law. Such consent must specify to a user the use of the data. It is then a matter for a user to decide whether they will allow or deny such access. The Guidelines provide that "Data collected for one purpose may not be repurposed without further consent unless otherwise explicitly permitted by law."

Sincerely,

Timothy Powderly

Timothy Powderly
Director, Federal Government Affairs
Apple