

March 2, 2012



VIA HAND AND EMIAL DELIVERY

The Honorable Henry A. Waxman
Ranking Member, Committee on Energy and Commerce
United States House of Representatives
Washington, D.C. 20515

The Honorable G.K. Butterfield
Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
United States House of Representatives
Washington, D.C. 20515

Dear Congressmen Waxman and Butterfield,

I am writing in response to your letter of February 15, 2012 regarding consumer privacy disclosures from application developers related to information contained in an iPhone address book.

I. Summary of Apple's Policies and Procedures

A. Apple's Commitment to Protecting our Customers' Privacy

Thank you for the opportunity to discuss consumer privacy issues. Apple is deeply committed to protecting the privacy of our customers who use our devices, and we are proud of our record. We have a single, comprehensive privacy policy for all of our products that can be reached from every page of our website. We have installed industry-leading features, including the "Find My iPhone" feature that can be used to erase personal data on an iPhone if lost or stolen, as well as making the default privacy setting on our browser, Safari, the most restrictive in the industry. We do not share personally identifiable information with third parties for their marketing purposes absent consent. As discussed more fully below, we require that third-party app developers that make apps available for download in our App Store abide by certain privacy guidelines.

Apple has an unwavering commitment to giving our customers clear and transparent notice, choice, and control over their personal information. For example, our software has a built in requirement for explicit user consent before an application can access location-based information. When an application requests the device location for the first time, a dialog box appears stating: "[Application] would like to use your current location." The customer is asked: "Don't Allow" or "Ok." If the customer clicks

“Don’t Allow,” no location-based information will be provided to the application. This dialogue box is mandatory – neither Apple’s applications nor those of third parties are permitted to override it. Similarly, we have announced that we will be enhancing explicit user consent to include contact data (Address Book) in a future software release.

B. Inclusion in the App Store

Your inquiry concerns, at least in part, the behavior of third-party application developers. In July 2008, Apple launched the App Store where customers can shop for and acquire applications offered by third-party developers. The App Store provides third-party developers a storefront from which they can market and sell their wares. Currently, the App Store has over 550,000 third-party applications covering a wide variety of areas including games, news, health, travel, education, business, sports, and social networking. The vast majority of these applications do not collect or transmit any user data whatsoever. And our privacy policy makes clear to our users that once a third-party application is downloaded to the user’s device, the user’s exchange of information with that third-party app is between the user and the app, and that the information exchange is governed by the privacy policy of the app.

Since July 2008, over 24 billion apps have been downloaded by customers using Apple devices. A recently completed economic analysis by TechNet shows that over 450,000 jobs have been created in the application development and deployment sector since the App Store was launched.¹

In order to offer an application for download in the App Store, a third-party developer must be registered as an “Apple Developer” and agree to the iOS Developer Agreement (the “IDA”) and the Program License Agreement (the “PLA”). Apple provides third-party developers with review guidelines, and conducts a review of all applications submitted for inclusion in the App Store for compliance with these documents.

The App Store Review Guidelines set forth the technical, design, and content guidelines Apple will use when reviewing an app for inclusion in the App Store. These guidelines state that apps “cannot transmit data about a user without obtaining the user’s prior permission and providing the user with access to information about how and where the data will be used.” This includes the transmission of personally identifiable information. In addition, the requirements of the PLA empower users to control access to user or device data, and require user consent before user or device data can be collected. The relevant portions of the PLA state that:

3.3.9. You and Your Applications may not collect user or device data without prior user consent, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising. You may not use analytics software in Your Application to collect and send device data to a third party.

¹ Available online at <http://www.technet.org/new-technet-sponsored-study-nearly-500000-app-economy-jobs-in-united-states-february-7-2012/> (accessed on February 21, 2012).

3.3.10. You must provide clear and complete information to users regarding Your collection, use and disclosure of user or device data. Furthermore, You must take appropriate steps to protect such data from unauthorized use, disclosure or access by third parties. If a user ceases to consent or affirmatively revokes consent for Your collection, use or disclosure of his or her user or device data, You must promptly cease all such use.

Other portions of the PLA address access to and use of location information, compliance with laws of general applicability (including privacy laws), and the protection of intellectual property. Apple receives over 26,000 applications for review each week, and approximately 30% are rejected for failure to comply with all of the developer guidelines. In most cases, the developer addresses the outstanding issue and resubmits the application.

C. Compliance

After the app is approved for inclusion in the App Store, a team of Apple employees is responsible for addressing any issues that arise. Apple conducts periodic random audits of apps that are in the App Store. Further, Apple routinely receives information about potential violations from users, competitors, developers, and other sources. When Apple becomes aware of a potential violation, such as an app not obtaining consent prior to accessing user data in an address book, Apple investigates, contacts the application developer, and if necessary, works with the developer to remedy the violation. If an application developer refuses to come in to compliance, the application will be expeditiously removed from the App Store. Apple has recently worked with Path and other third-party application developers to ensure that our users receive accurate notice about the developers' request for access to users' address books.

II. Responses to the Written Questions

- 1. Please describe all iOS App Guidelines that concern criteria related to the privacy and security of data that will be access or transmitted by an app.**

For Apple's response to this question, please see the "Apple's Commitment to Protection our Customers' Privacy" and "Inclusion in the App Store" sections above.

- 2. Please describe how you determine whether an app meets those criteria.**

For Apple's response to this question, please see the "Inclusion in the App Store" section above.

3. **What data do you consider to be “data about a user” that is subject to the requirement that the app obtain user consent before it is transmitted?**

For Apple’s response to this question, please see the “Inclusion in the App Store” section above.

4. **To the extent not addressed in response to question 2, please describe how you determine whether an app will transmit “data about a user” and whether the consent requirement has been met.**

For Apple’s response to this question, please see the “Inclusion in the App Store” and “Compliance” sections above.

5. **How many iOS apps in the U.S. iTunes Store transmit “data about a user”?**

For Apple’s response to this question, please see the “Inclusion in the App Store” section above.

6. **Do you consider the contents of the address book to be “data about a user”?**

For Apple’s response to this question, please see the “Compliance” section above.

7. **Do you consider the contents of the address book to be data of the contact? If not, please explain why not. Please explain how you protect the privacy and security interests of that contact in his or her information.**

For Apple’s response to this question, please see the “Inclusion in the App Store” section above.

8. **How many iOS apps in the U.S. iTunes Store transmit information from the address book? How many of those ask for the user’s consent before transmitting their contacts’ information?**

For Apple’s response to this question, please see the “Inclusion in the App Store” and “Compliance” sections above.

9. **You have built into your devices the ability to turn off in one place the transmission of location information entirely or on an app-by-app basis. Please explain why you have not done the same for address book information.**

For Apple's response to this question, please see the "Apple's Commitment to Protecting our Customers' Privacy" section above.

Let me restate Apple's unwavering commitment to giving our customers clear and transparent notice, choice, and control over their personal information. We believe our products do this in a simple and elegant way and we work to continually improve our customers' experience in this regard. We appreciate this opportunity to explain our policies and procedures to you.

Sincerely,



Catherine A. Novelli
Vice President, Worldwide Government Affairs