

November 1, 2013



VIA ELECTRONIC AND HAND DELIVERY

The Honorable Al Franken
United States Senate
Chairman
Senate Judiciary Subcommittee
On Privacy, Technology, and the Law
224 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Franken,

I am writing in response to your letter of September 19, regarding the privacy and security features of Touch ID. Touch ID is a fingerprint identity sensor embedded onto iPhone 5s, which provides a convenient and highly secure way for customers to unlock their iPhones.

Throughout its history, Apple has prioritized consumer privacy by designing privacy protection and leading-edge user controls into the fabric of its products and services. For example, Apple was the first mobile platform to allow users to opt-out of certain targeted advertising using Limit Ad Tracking, a simple toggle setting on their devices. Apple now also rejects apps that require access to persistent device identifiers, which distinguishes it from other companies. Apple also pioneered technology called “sandboxing,” which limits individual apps’ access to information stored in other apps on the mobile device.

Apple has adopted a single comprehensive privacy policy for all its businesses and products, including the iTunes Store and the App Store. We are committed to providing our customers with clear notice, choice and control over their information. Touch ID is a good example of how Apple proactively embedded customer privacy and security protection into its products.

Set forth below are answers to the questions raised in your letter.

1. Is it possible to convert locally-stored fingerprint data into a digital or visual format that can be used by third parties?

No, the data is encrypted and securely stored in the Secure Enclave on Apple’s all-new A7 chip on the iPhone 5s. The data stored in the Secure Enclave on the customer’s device is a derivative mathematical model that cannot be used to construct a digital or visual representation of the scanned image. iOS does not have access to Secure Enclave data. The model is never stored on Apple servers or backed-up to iCloud.

2. Is it possible to extract and obtain fingerprint data from an iPhone? If so, can this be done remotely, or with physical access to the device?

No.

3. In 2011, security researchers discovered that iPhones were saving an unencrypted file containing detailed historical location information on the computers used to back up the

device. Will fingerprint data be backed up to a user's computer?

No.

4. Does the iPhone 5S transmit any diagnostic information about the Touch ID system to Apple or any other party? If so, what information is transmitted?

Yes, if a user opts-in to diagnostic data submissions, information about the general performance and usage of the Touch ID sensor may be submitted to Apple. The data is only submitted to Apple and not shared with third parties. No personal or fingerprint data is collected.

5. How exactly do iTunes, iBooks and the App Store interact with Touch ID? What information is collected by those apps from the Touch ID system, and what information is collected by Apple associated with those interactions, including identifiers or hashes related to fingerprint data?

If a customer chooses to use Touch ID to approve purchases, Touch ID locally verifies that it matches an authorized finger for that purchase. The customer's iPhone 5s then submits the fact that a match occurred to Apple's servers, allowing Apple servers to approve the purchase. No identifiers or hashes related to the fingerprint data used for this interaction are collected by Apple.

6. Does Apple have any plans to allow any third party applications access to the Touch ID system or its fingerprint data?

Apple does not discuss plans for future products, features, or services. But, third party applications do not have access to the Touch ID system or its fingerprint data.

7. Can Apple assure its users that it will never share their fingerprint data, along with tools or other information necessary to extract or manipulate the iPhone fingerprint data, with any commercial third party?

The locally-stored fingerprint data is contained within Apple's A7 Secure Enclave on the customer's device and is not available to third parties.

8. Can Apple assure its users that it will never share their fingerprint data, along with tools or other information necessary to extract or manipulate the iPhone fingerprint data, with any government, absent appropriate legal authority and process?

Yes.

9. Under American privacy law, law enforcement agencies cannot compel companies to disclose the "contents" of communications without a warrant, and companies cannot share that information with third parties without customer consent. However, the "record[s] or other information pertaining to a subscriber... or customer" can be freely disclosed to any third party without customer consent, and can be disclosed to law enforcement upon issuance of a non-probable cause court order. Moreover, a "subscriber number or identity" can be disclosed to the government with a simple subpoena. See generally 18 U.S.C. § 2702-2703.

Does Apple consider fingerprint data to be the “contents” of communications, customer or subscriber records, or a “subscriber number or identity” as defined in the Stored Communications Act?

As explained above, Apple does not collect fingerprint data from customer’s devices. Instead the locally-stored fingerprint data is only available to Apple’s A7 Secure Enclave on the customer’s device. Thus, the above question does not apply to this data.

10. Under American intelligence law, the Federal Bureau of Investigation can seek an order requiring the production of “any tangible thing[] (including books, records, papers, documents and other items)” if they are deemed relevant to certain foreign intelligence investigations. See 50 U.S.C. § 1861.

Does Apple consider fingerprint data to be “tangible things” as defined in the USA PATRIOT Act?

As explained above, Apple does not collect fingerprint data from customer’s devices. Instead the locally-stored fingerprint data is only available to Apple’s A7 Secure Enclave on the customer’s device. Thus, the above question does not apply to this data.

11. Under American intelligence law, the Federal Bureau of Investigation can unilaterally issue a National Security Letter that compels telecommunications providers to disclose “subscriber information” or “electronic communication transactional records in its custody or possession.” National Security Letters typically contain a gag order, meaning that recipients cannot disclose that they received the letter. See, e.g., 18 U.S.C. § 2709.

Does Apple consider fingerprint data to be “subscriber information” or “electronic communication transactional records” as defined in the Stored Communications Act?

As explained above, Apple does not collect fingerprint data from customer’s devices. Instead the locally-stored fingerprint data is only available to Apple’s A7 Secure Enclave on the customer’s device. Thus, the above question does not apply to this data.

12. Does Apple believe that users have a reasonable expectation of privacy in fingerprint data they provide to Touch ID?

Yes. Because the fingerprint data is only available to Apple’s A7 Secure Enclave on the customer’s device and given that the fingerprint data is a derivative mathematical model that cannot be used to construct a digital or visual representation of the skin area scanned, we believe that this data would be considered non-public for which the customer would have a reasonable expectation of privacy.

Sincerely,



Bruce Sewell
Senior Vice President and General Counsel