

PATRICK J. LEAHY, VERMONT, CHAIRMAN

DIANNE FEINSTEIN, CALIFORNIA
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
SHELDON WHITEHOUSE, RHODE ISLAND
AMY KLOBUCHAR, MINNESOTA
AL FRANKEN, MINNESOTA
CHRISTOPHER A. COONS, DELAWARE
MAZIE HIRONO, HAWAII

CHARLES E. GRASSLEY, IOWA
ORRIN G. HATCH, UTAH
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TED CRUZ, TEXAS
JEFF FLAKE, ARIZONA

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

BRUCE A. COHEN, *Staff Director*
KRISTINE J. LUCIUS, *Chief Counsel and Deputy Staff Director*
KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*
RITA LARI JOCHUM, *Republican Deputy Staff Director*

September 19, 2013

Mr. Tim Cook, CEO
Apple, Inc.
1 Infinite Loop
Cupertino, CA

Dear Mr. Cook:

I am writing regarding Apple's recent inclusion of a fingerprint reader on the new iPhone 5S. Apple has long been a leading innovator of mobile technology; I myself own an iPhone. At the same time, while Apple's new fingerprint reader, Touch ID, may improve certain aspects of mobile security, it also raises substantial privacy questions for Apple and for anyone who may use your products. In writing you on this subject, I am seeking to establish a public record of how Apple has addressed these issues internally and in its rollout of this technology to millions of my constituents and other Americans.

Too many people don't protect their smartphones with a password or PIN. I anticipate that Apple's fingerprint reader will in fact make iPhone 5S owners more likely to secure their smartphones. But there are reasons to think that an individual's fingerprint is not "one of the best passwords in the world," as an Apple promotional video suggests.

Passwords are secret and dynamic; fingerprints are public and permanent. If you don't tell anyone your password, no one will know what it is. If someone hacks your password, you can change it – as many times as you want. You can't change your fingerprints. You have only ten of them. And you leave them on everything you touch; they are definitely *not* a secret. What's more, a password doesn't uniquely identify its owner – a fingerprint does. Let me put it this way: if hackers get a hold of your thumbprint, they could use it to identify and impersonate you for the rest of your life.

It's clear to me that Apple has worked hard to secure this technology and implement it responsibly. The iPhone 5S reportedly stores fingerprint data locally "on the chip" and in an encrypted format. It also blocks third-party apps from accessing Touch ID. Yet important questions remain about how this technology works, Apple's future plans for this technology, and the legal protections that Apple will afford it. I should add that regardless of how carefully Apple implements fingerprint technology, this decision will surely pave the way for its peers and smaller competitors to adopt biometric technology, with varying protections for privacy.

I respectfully request that Apple provide answers to the following questions:

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

- (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?
- (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?
- (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?
- (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 the fingerprint data?
- (6) Does Apple have any plans to allow any third party applications 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?
- (8) Can Apple assure its users that it will never share their fingerprint files, along with tools or other information necessary to extract or manipulate the iPhone fingerprint data, with any government, absent appropriate legal authority and process?
- (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?

- (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?


- (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?

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

Thank you for your time and attention to these questions. I ask that Apple answer these questions within a month of receiving this letter.

Sincerely,



Al Franken
Chairman, Senate Judiciary Subcommittee
on Privacy, Technology and the Law