

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*

May 13, 2014

Dr. Oh-Hyun Kwon, CEO
Samsung Electronics Co., Ltd.
Samsung Main Building
250, Taepyeongno 2-ga, Jung-gu
Seoul, 100-742, Korea

Mr. Gregory Lee, CEO
Samsung Electronics North America
85 Challenger Road
Ridgefield Park, NJ 07660

Dear Dr. Kwon and Mr. Lee:

I am writing to ask you about privacy protections for the fingerprint scanning technology on the Samsung Galaxy S5 smartphone, which recently went on sale. I am concerned by reports that Samsung's fingerprint scanner may not be as secure as it may seem – and that those security gaps might create broader security problems on the S5 smartphone.¹ I am writing to request information on how Samsung is addressing these and other privacy questions about its fingerprint scanner.

The security benefits of fingerprint technology are not as clear as many would expect. On the one hand, it's easier to swipe your finger than to tap out a complex password. Thus, the convenience of the fingerprint scanner may result in more smartphone owners actually locking their phones. On the other hand, fingerprint scanners raise acute security problems that passwords do not – particularly when they are used *instead of* rather than *in addition to* password verification. As I explained in an earlier letter to Apple regarding their rollout of their Touch ID fingerprint scanner, passwords are secret and dynamic, while fingerprints are public and permanent. If you don't tell anyone your password, no one will know it. If it gets hacked, you can change it in a minute or two.

Fingerprints are the opposite of secret. You leave them on countless objects that you touch throughout the day: your car door, a glass of water, even the screen of your smartphone. And unlike passwords, fingerprints cannot be changed. If hackers get hold of a digital copy of your fingerprint, they could use it to impersonate you for the rest of your life, particularly as more and more technologies start relying on fingerprint authentication.

¹ See, e.g., Dan Goodin, *Fingerprint lock in Samsung Galaxy 5 easily defeated by whitehat hackers*, Ars Technica, April 15, 2014.

Like Apple's Touch ID, the Galaxy S5's fingerprint scanner was hacked a few days after the smartphone's release. Security researchers bypassed both scanners by creating a fake rubber print from a fingerprint lifted *from the screen of a smartphone*.²

Initial reports also suggest that the Galaxy S5 may raise security concerns that Touch ID does not. The Galaxy S5 fingerprint scanner reportedly allows for unlimited authentication attempts without a password prompt, whereas Apple's Touch ID requires a password after only five failed attempts.³ Furthermore, while Touch ID can be used only to unlock a device and to access certain tightly monitored Apple apps, Galaxy S5 appears to allow any app to use the fingerprint scanner instead of a password.⁴ This means that you can use the Galaxy S5 fingerprint scanner to send money on PayPal and access your password app; unfortunately, it likely means that bad actors who spoof your fingerprints can do that, too. This broader access to the scanner could potentially allow third parties to access sensitive information generated by the technology.

I respectfully request that Samsung provide answers to the following questions. All but the first are almost identical to the questions I posed to Apple last year.

- (1) How exactly does Samsung secure the fingerprint data generated by the Galaxy S5's fingerprint scanner?
- (2) Is it possible to convert locally-stored fingerprint data into a digital or visual format that can be used by third parties?
- (3) Is it possible to extract and obtain fingerprint data from a Galaxy S5? If so, can this be done remotely, or with physical access to the device?
- (4) Will fingerprint data be backed up to a user's computer? Will fingerprint data be backed up to the cloud or to Samsung servers?
- (5) Does the Galaxy S5 transmit any diagnostic information about the fingerprint scanner system to Samsung or any other party? If so, what information is transmitted?
- (6) How exactly do Samsung apps and third party apps interact with the fingerprint scanner? What information is collected by those apps from the fingerprint scanner system, and what information is collected by Samsung associated with those interactions, including identifiers or hashes related to the fingerprint data?
- (7) What are Samsung's future plans for fingerprint scanning technology? Will it deploy the technology on its tablet devices, as news reports suggest?

² See SRLabs, *Samsung Galaxy S5 Finger Scanner also susceptible to ordinary spoofs*, YouTube, April 15, 2014; SRLabs, *iPhone 5s Touch ID susceptible to fingerprint spoofs*, YouTube, Sept. 25, 2013.

³ See *supra* note 1; Apple, *iPhone 5s: Using Touch ID*, available at <http://support.apple.com>.

⁴ See *generally Samsung Mobile SDK*, available at <http://developer.samsung.com>.

- (8) Can Samsung assure its users that it will never share their fingerprint data, along with tools or other information necessary to extract or manipulate the Galaxy S5 fingerprint data, with any commercial third party?
- (9) Can Samsung assure its users that it will never share their fingerprint data, along with tools or other information necessary to extract or manipulate the Galaxy S5 fingerprint data, with any government, absent appropriate legal authority and process?
- (10) 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 Samsung 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?

- (11) 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 Samsung consider fingerprint data to be “tangible things” as defined in the USA PATRIOT Act?

- (12) 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 Samsung consider fingerprint data to be “subscriber information” or “electronic communication transactional records” as defined in the Stored Communications Act?

- (13) Does Samsung believe that users have a reasonable expectation of privacy in fingerprint data they provide to the fingerprint scanner?

I’m not trying to discourage adoption of fingerprint technology for consumer mobile devices. If adopted with strong safeguards, this technology could prove to be convenient and beneficial. Rather, my goal is to urge companies to deploy this technology in the most secure manner reasonable – and create a public record around how companies are treating sensitive biometric information.

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

Sincerely,

A handwritten signature in blue ink, appearing to read "Al Franken". The signature is fluid and cursive, with a long horizontal stroke at the end.

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