



SAMSUNG TELECOMMUNICATIONS AMERICA, LLC
1301 E. Lookout Dr.
Richardson, TX 75082 U.S.A.
TEL 972-761-7000

June 12, 2014

The Honorable Al Franken
309 Hart Senate Office Building
United States Senate
Washington, DC 20510

Dear Senator:

Thank you for your letter of May 13 to Samsung Electronics. Samsung is a world leader in consumer technology innovation, and we honor and value the trust that consumers have in our products. We agree with you that fingerprint scanning technology for smartphones can be convenient and beneficial for consumers but must be implemented in a way that safeguards consumer privacy.

We appreciate the opportunity to respond to your questions about how we have implemented fingerprint scanning technology in our Galaxy S5 smartphones. Please see our attached responses to each of your questions and to one additional point raised within your letter. If you should have any additional questions, please contact me at the number or email below or Joel Wiginton in our Washington, DC office at 202-552-3021 or j.wiginton@sea.samsung.com.

With sincere regards,

A handwritten signature in blue ink that reads "Cindi Moreland".

Cindi Moreland
Vice President & General Counsel
972-761-7060
cmoreland@sta.samsung.com

Attachment



SAMSUNG TELECOMMUNICATIONS AMERICA, LLC
1301 E. Lookout Dr.
Richardson, TX 75082 U.S.A.
TEL 972-761-7000

Questions and Responses

- 1) How exactly does Samsung secure the fingerprint data generated by the Galaxy S5's fingerprint scanner?

The scanner does not store the fingerprint image. Instead, it stores a mathematical representation of the image (plots of endpoints and curvatures), which cannot be converted back to the fingerprint image. The mathematical representation is stored in a secure part of the semiconductor architecture and cannot be accessed by or shared with external sources. It remains inside the phone.

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

As stated in the response to Question 1, the scanner does not store the image, and the mathematical representation cannot be converted back to the actual image.

- 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?

As stated in the response to Question 1, the mathematical representation is stored in a secure part of the semiconductor architecture and is protected against access from external sources, including remote 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?

As stated in the response to Question 1, the mathematical representation is only stored in the phone. It is not transferred to a user's computer, the cloud, or 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?

There are no diagnostic capabilities in the fingerprint scanner application; therefore, no diagnostic information data is collected or transmitted to any parties.

- 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?



SAMSUNG TELECOMMUNICATIONS AMERICA, LLC
1301 E. Lookout Dr.
Richardson, TX 75082 U.S.A.
TEL. 972-761-7000

The scanner is only used for biometric identification. The scanner has a very limited interaction with other Samsung applications and applications from third parties. Specifically, when an application requires authentication of the user, the application directs the scanner to prompt the user to input his or her fingerprint; the scanner checks the scan against the internally stored mathematical representation of the authorized user's fingerprint; and the scanner returns only a "yes" (matching) or "no" (not matching) response to the application. The application does not have access to the user's fingerprint or the mathematical representation of the user's fingerprint.

- 7) What are Samsung's future plans for fingerprint scanning technology? Will it deploy the technology on its tablet devices, as news reports suggest?

We can expand and evolve our fingerprint scanner application to meet diverse consumer needs. We are currently developing the product strategy for the fingerprint scanning application beyond the Galaxy S5.

- 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?

The hardware and software architecture prevents sharing of fingerprint data with third parties, and we do not have tools to extract or manipulate the fingerprint data from the Galaxy S5.

- 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?

Same as response to Question 8.

- 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] of 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?

It does not appear that the Stored Communication Act ("SCA") applies to Samsung because, as stated in our responses above, fingerprint data generated by our fingerprint scanner is stored in a secure location on the device and is protected from outside access, and the data is neither transferred nor shared for the purpose of providing "electronic communications services" or "remote computing services." Most courts that have considered the issue have held that the SCA does not apply to access to information stored on a mobile device because a mobile device is not a “facility” through which an “electronic communications service” is provided. See *In re iPhone Application Litigation*, 844 F.Supp.2d 1040, 1057 (N.D.Cal. 2012); *U.S. v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003); *Freedom Banc Mortg. Servs., Inc. v. O’Harra*, No. 2:11-CV-01073, 2012 U.S. Dist. LEXIS 125734 at *23 (S.D. Ohio, Sept. 5, 2012); but see *Cousineau v. Microsoft Corp.*, No. C11-1438-JCC (W.D. Wa., June 22, 2012). At this time, Samsung does not have an independent view regarding how the law applies to other companies that might fall within its scope.

- 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?

Because fingerprint data generated by the fingerprint scanner on Samsung devices is stored locally on the customer’s device and is not in the possession of Samsung, Samsung has no independent view regarding whether that data would be considered “tangible things” by the holder of that information for purposes of an order under 50 U.S.C. § 1851.

- 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.



SAMSUNG TELECOMMUNICATIONS AMERICA, LLC
1301 E. Lookout Dr.
Richardson, TX 75082 U.S.A.
TEL 972-761-7000

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

It does not appear that the SCA applies to Samsung in this scenario for the reasons set forth in our response to Question 10 above and the case law cited therein. At this time, Samsung does not have an independent view regarding how the law applies to other companies that might fall within its scope.

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

Yes. We believe that, as a general matter, users have a reasonable expectation of privacy in fingerprint data they choose to store on their devices using the fingerprint scanner. As stated in our responses above, Samsung has implemented reasonable security measures to protect fingerprint data that users choose to store on their devices, including saving the data to a protected section of the device to prevent external access.

Other

We would like to correct your understanding of the automatic blocking feature following a series of non-matching fingerprint inputs by the user, as you discussed in your letter. Galaxy S5’s fingerprint scanner does provide for automatic blocking, which operates per the following schedule:

- After 5 incorrect inputs: 30 second block**
- After 10 incorrect inputs: Additional 30 second block**
- After 15 incorrect inputs: Additional 30 second block**
- After 20 incorrect inputs: Consumer must input password to proceed**