The Washington Post

The Switch • Analysis

Apple is opening up amid privacy questions about Face ID, personal data collection

By Hayley Tsukayama September 27

Apple released more details about the iPhone X's Face ID feature when it published a new privacy site Wednesday, addressing some of the concerns that people have had since the face-scanning feature was announced.

When Apple unveiled the feature, which can unlock phones and be used for payments, it spurred not only a thousand alarming think pieces, but also a letter from Sen. Al Franken (D-Minn.) asking how the company will protect the data. There have also been worries about how much to trust Face ID. The company's first public demo of Face ID didn't go that smoothly, after all — at one point, the demonstrator had to skip the face scan and enter his password instead.

The most telling answers on Face ID come from a white paper the company's posted on its security.

The information collected by Face ID won't leave your device, the company reiterates on the site. Apple also lays out exactly what it's storing: infrared images of your face captured when you first start Face ID, the mathematical representations of your face it calculates during that enrollment and whatever other images the phone deems necessary to account for changes to your face (a beard growing over time, for example). Images are also cropped close to your face to avoid grabbing any background information.

There are also several instances when Face ID won't work. These include when:

- The device has just been turned on or restarted.

- The device hasn’t been unlocked for more than 48 hours.

- The passcode hasn’t been used to unlock the device in the past 156 hours (6 ½ days) and Face ID has not unlocked the device in the past four hours.

- The device has received a remote lock command.

- There have been five unsuccessful attempts to match a face. (Note: This is what happened onstage to Apple's head of software, Craig Federighi, when he demonstrated the feature for the first time in public after others handled the demo phone.)

- You power off or initiate the Emergency SOS by pressing and holding either volume button and the side button simultaneously for two seconds.

This last tip, at least in part, addresses concerns that people will not be able to stop others from using Face ID to open an individual's phone without consent. And by activating the Emergency SOS, you'll also be dialing an emergency number and disabling the Touch ID and Face ID features. That should help users worried about being asked to open their phones under duress, such as while being mugged. That is, if they have the time to activate it when needed.

Apple's new privacy site also breaks down its practices on everything from Apple Pay to encryption to health data on the site, offering short descriptions of how it uses data, how it protects data and often adds links to give those interested in more information on its policies. It's a comprehensive website and more reader-friendly than any other tech giant's privacy center. Still, it's a lot of reading and a reminder of all the information we're entrusting to Apple and its philosophies on data protection.

Overall, what really may be most useful for people looking at this site is the articulation from Apple about how it views privacy as they push further into personal wearable devices and home hubs. The fact that it's made this knowledge center at all shows that it will continue to try to provide more personalized services with a privacy bent.