Forbes

Apple Claims It Encrypts iMessages And Facetime So That Even It Can't Decipher Them

By: Andy Greenberg - June 17, 2013

In the wake of the revelation of the National Security Agency's PRISM surveillance program, tech companies have scrambled to counter claims that they give the government direct backdoor access to their servers. But Apple has taken the opportunity to make a bolder claim: That even the company itself can't read many of the communications between its users.

"Apple has always placed a priority on protecting our customers' personal data, and we don't collect or maintain a mountain of personal details about our customers in the first place," reads a statement it published late Sunday night on its website. "There are certain categories of information which we do not provide to law enforcement or any other group because we choose not to retain it. For example, conversations which take place over iMessage and FaceTime are protected by end-to-end encryption so no one but the sender and receiver can see or read them. Apple cannot decrypt that data."

Apple also argued that many of its services don't store any data that would be available to government requests. "We do not store data related to customers' location, Map searches or Siri requests in any identifiable form," its statement reads.

Apple's message did reveal some information about how often it hands customers' data over to the federal government, writing that it had received between 4,000 and 5,000 requests for data from 9,000 to 10,000 of its users' accounts in the first six months of 2013. It claimed that those requests were mostly intent on "searching for missing children, trying to locate a patient with Alzheimer's disease, or hoping to prevent a suicide," but could also include national security issues. In separate reports over the weekend, Facebook and Microsoft released similar data from late 2012, revealing that Microsoft had responded to government requests for 31,000-32,000 users' accounts in that period, and Facebook had dealt with requests for beteween 18,000 and 19,000.

Regardless, those numbers only seem to cover law enforcement requests, and may not include the special Foreign Intelligence Surveillance Act (FISA) court orders that would provide data to the NSA. Google, for instance, has for years published the number of times it gives user data to law enforcement in a bi-annual report, but In the wake of media attention to the PRISM program is still requesting special permission from U.S. Attorney General Eric Holder and FBI Director Robert Mueller to publish those FISA orders.

Apple's revelation that it can't decrypt–and in many cases doesn't store–key customer data and communications, however, comes as more surprising distinction among the tech companies.

Other firms including Google and Facebook that offer instant messaging haven't publicly claimed that use so-called "end-to-end" encryption. Many firms such as Dropbox that do claim to encrypt users' data still hold the decryption key themselves, which would allow the company to read users' private information when required to by law. And Skype, whose service is similar to the FaceTime software Apple offers, raised the ire of privacy advocates last July when it refused to comment on whether it can or does eavesdrop on users' conversations on behalf of law enforcement.

The relative security of Apple's iMessage service first came to light earlier this year, when Cnet published an internal Drug Enforcement Agency memo that claimed "it is impossible to intercept iMessages between two Apple devices" due to their encryption, even when a judge has issued a warrant for the surveillance. The agency wrote that it could read text messages sent between iMessage and a non-Apple phones, however, and suggested that "the outcome seems to be more successful if the intercept is placed on the non-Apple device."

Privacy advocates at the time cautioned users against relying on that purported iMessage security. Julian Sanchez, a research fellow with the Cato Institute, for instance, warned that "…the cloud provider must itself hold the keys to unlock that data. So iMessages may not be interceptable from a suspect's cell carrier, but Apple has to be capable of handing them over when the authorities come knocking with a warrant."

Apple's newest claims seem to directly counter that argument. But just because Apple can't decrypt users' communications doesn't mean the NSA can't. John Hopkins University cryptographer Matthew Green last year wrote a blog post about iMessage's encryption, arguing that it needed more scrutiny before it could be declared secure. "Apple [operates] one of the most widely deployed encrypted text message services in the history of mankind," he wrote. "The problem is that they still won't properly explain how it works."

Apple, after all, hasn't made its cryptographic protocols available to the public, unlike other encrypted messaging services such as Whisper Systems or CryptoCat. Green went on to note just how complicated and obscure iMessage's inner workings are, which may provide a foothold for governments to surreptitiously eavesdrop on users' communications. "

As a general rule, lots of moving parts means lots of places for things to go wrong," he wrote. "Things that could seriously reduce the security of the protocol. And as far as I know, nobody's given this much of a look."

In other words, Apple may not be decrypting your conversations and handing them directly to a government agency. But iMessaging or FaceTiming with your drug dealer, Deep Throat, or criminal co-conspirator still probably isn't the wisest move.