Apple’s Commitment to Customer Privacy

Two weeks ago, when technology companies were accused of indiscriminately sharing customer data with government agencies, Apple issued a clear response: We first heard of the government’s “Prism” program when news organizations asked us about it on June 6. We do not provide any government agency with direct access to our servers, and any government agency requesting customer content must get a court order.

Like several other companies, we have asked the U.S. government for permission to report how many requests we receive related to national security and how we handle them. We have been authorized to share some of that data, and we are providing it here in the interest of transparency.

From December 1, 2012 to May 31, 2013, Apple received between 4,000 and 5,000 requests from U.S. law enforcement for customer data. Between 9,000 and 10,000 accounts or devices were specified in those requests, which came from federal, state and local authorities and included both criminal investigations and national security matters. The most common form of request comes from police investigating robberies and other crimes, searching for missing children, trying to locate a patient with Alzheimer’s disease, or hoping to prevent a suicide.

Regardless of the circumstances, our Legal team conducts an evaluation of each request and, only if appropriate, we retrieve and deliver the narrowest possible set of information to the authorities. In fact, from time to time when we see inconsistencies or inaccuracies in a request, we will refuse to fulfill it.

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. 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. Similarly, we do not store data related to customers’ location, Map searches or Siri requests in any identifiable form.

We will continue to work hard to strike the right balance between fulfilling our legal

responsibilities and protecting our customers’ privacy as they expect and deserve.