Apple's Commitment to Customer Privacy

June 16, 2013

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.

Explication:

Balancing Privacy and Legal Responsibilities: Apple's Case

In the digital area we live in, protecting private information has become one of the most crucial ethical dilemmas facing companies. As people use technology for communication, work, and entertainment, companies that store their data need to keep it safe. This case illustrates how the tech giant Apple, one of the most valuable companies in the world, responded to accusations about sharing customer data with the U.S. government, and the privacy implications, and trust-reliant industry.

In 2013, reports surfaced about a government surveillance program known as “Prism,” putting Apple in the spotlight. The program was reported to have provided government agencies with direct access to data held by major technology companies including Apple, Google, and Facebook. Apple, however, was quick to deny these claims. The company said that it first learned of “Prism” from news reports and added that it does not permit any government agency to directly access its servers. Apple also made a point to remind users that based on their guidelines a request for information must be backed by a court order before sharing information, all of which is very good news for consumers.

Over the six months between December 2012 and May 2013, Apple received 4,000 to 5,000 law enforcement requests. These involved data from 9,000 to 10,000 accounts or devices. The requests were often made by police officers investigating crimes, searching for missing people, or managing public safety issues like forestalling suicides. Apple said it evaluated each request closely and provided only the minimum information required. Apple also pointed out that some of its services, including iMessage and FaceTime, have end-to-end encryption. This kind of encryption guarantees the messages can be accessed only by the sender and the recipient, not even Apple itself can read them.

From the customers' point of view, this posed a lot of privacy issues. While Apple said it had processed data requests responsibly, that left many concerned about how much personal information may still be obtainable. Others were worried about the possibility of their data being passed around without their knowledge, even if it was for law enforcement reasons. With the potential for people to be surveilled,

either by the government or through their interactions with technology, people couldn't be sure their private lives were private. This case raised questions of trust: How much can customers trust companies to safeguard their information? And what level of power should governments have in accessing personal data in the name of security?

From Apple's point of view, the company finally made some moves to demonstrate it cared about privacy. Apple said it acted legally but also sought to protect its customers. It would only share data, when it was legally obligated to do so, and if the requests were legitimate. By examining each request in extensive detail, Apple wanted to prevent unnecessary violations of privacy. Also, Apple's use of encryption for services such as iMessage and FaceTime showed its attempts to make some data completely unavailable, even with a legal request. Apple also encouraged transparency by revealing how many data requests it received, and it pressed the government to allow companies to be more forthcoming about such requests. With these moves, Apple tried to assure customers that it cared about their privacy above all.

It underscores the friction that remains between companies' legal obligations and the moral commitment to keep users' personal information secure. Apple et al. have a duty to obey the law and to assist law enforcement when the law requires such assistance, but they also need to maintain customer faith by protecting their privacy to the greatest degree possible. Open communication and policy clarity are essential to striking this balance. Asking Apple how many requests it received, and then explaining how it handled those requests, was fresh air — especially when it was refreshing this little-blip-on-the-radar post-lunch afternoon two weeks ago.

Ultimately, Apple's case demonstrates how technology companies can wrestle with those knotty privacy problems that we face today in the digital world. Customers may still have concerns about how their

data is used, but Apple's method of balancing legal compliance with privacy-first protections illustrates that government requirements and individual rights can coexist. Striking this balance is crucial to instilling trust in and ethical use of personal information in our ever-connected world.

Source: "Apple Statement on Customer Privacy," June 16, 2013