AppleScare

One of the most enduring and fraught discussions centering upon privacy and technology is the practice of encrypting messages and files on mobile devices. We are promised that our personal devices are entirely private. At the same time, tech companies are struggling with the demands of governments to give access to the data circulating on our phones.

Law enforcement officials have frequently submitted legal orders to major tech companies such as Apple, Google, and Microsoft to hand over the contents of messages, photos, and files on consumers' phones for criminal investigations. Yet, not all data on our phones is so easily accessible. In the interest of protecting user privacy, and perhaps out of concern for governmental abuse (whether by the United States or foreign entities), software developers created “end-to-end” encrypted chat apps (e.g. WhatsApp, Snapchat). These apps secure and hide the contents of a message until it reaches the other user’s phone. Only the two end users hold the decryption key; as a result, the phone-maker does not have the ability to hand over data because it was never readable on their servers in the first place.

Law enforcement and government officials have claimed emphatically that disclosures of user data are necessary to combat terrorism, assure national security, and curb violent crime. One such area of concern is systemic child trafficking and child pornography.

In the spring of 2021, Apple disturbed the waters of this uneasy truce over encrypted communication. The tech giant partnered with the National Center for Missing & Exploited Children to formulate a way to scan the hard drives of iPhones for known “Child Sexual Abuse Material” (CSAM). This practice, first employed in limited contexts by the FBI, converts each known image of CSAM in its database into a unique numerical identifier. Meanwhile, every iPhone will regularly run the same algorithm—behind the scenes—to likewise convert files and photos on phones into numeric values. If there is a numeric match between the CSAM database and a file on a user’s phone, it raises a red flag to Apple that the phone owner is in possession of problematic material.

Apple insists that its software and algorithm does not “see” user images. Instead, the algorithm blindly converts images to numerical values (called a “hash”) and then simply looks for matches between user files and hashes in the criminal database. Thus, according to Apple, parents who take pictures of their infant children taking a bath, for instance, have nothing to worry about, because such pictures will not correspond to any pattern of known CSAM.

DISCUSSION QUESTIONS

1. How can tech companies reconcile the demands of law enforcement agencies with the demands of users for privacy?
2. To what degree, if at all, should government agencies be trusted with looking over our “private” data?
3. The same messaging encryption which lets investigative journalists communicate safely is also employed by violent criminals and terrorist actors. Is such encryption necessary for a free society? Is it a danger to social stability?