Case #1: Apple vs. FBI

The dispute between Apple Inc. and the Federal Bureau of Investigation (FBI) has, once again, brought to public attention the tension between privacy and national security. After the 2015 San Bernardino shooting, the FBI ordered Apple to provide anti-encryption software to access the information locked inside an iPhone 5c belonging to one of the shooters. In February of 2016, Apple publicly refused to comply with the Federal order, citing the protection of customers’ data from “hackers and criminals” and noting that they even “put that data out of our own reach” because it is “none of our business.” It is unclear precisely what information the FBI might be interested in on the shooter’s phone, but the encrypted information included emails, calendar data, text messages, photos, and contacts.

A host of tech companies, like Yahoo! and Facebook, along with the American Civil Liberties Union, publicly supported Apple’s position. Even the U.N. Human Rights Chief expressed dismay for the FBI order, citing “the potential for ‘extremely damaging implications’ on human rights, journalists, whistle-blowers, political dissidents and others.” He said such an order is “potentially a gift to authoritarian regimes.”

On the other hand, families of victims and attack survivors have criticized Apple’s intransigence. Victims’ families and friends are concerned that setting obstacles for the investigation hinders their chance at closure as well as finding accomplices to the crimes. “Let’s see how you feel when it affects you,” said one person, whose boyfriend was killed in the attack. According to the executive director of the National Sheriff’s Association, Jonathan Thompson, Apple’s refusal to comply with FBI’s orders puts “profit over safety.” “This has nothing to do with privacy,” he continued, “It’s all about money and their brand.” Federal authorities say they are concerned with national security. They contend that such encryption technologies make it more difficult for them to solve cases and prevent terrorist attacks. In response to concerns about the government overstepping its bounds, officials say this is a “one-off request” and should not be regarded as setting a precedent. Decisions about which information to gather and from whom are not taken lightly and follow strict protocols before an

---

investigation proceeds. The FBI concluded that Apple’s concern for its customers’ privacy cannot legitimately justify obstructing the pursuit of threats to public safety.

Case from the 2016 Regional Ethics Bowls
© Association for Practical and Professional Ethics 2016