Challenging Technology

Should Apple hack for the ‘good guys?’

Thursday, February 25, 2016

On Feb. 16, a federal judge ordered Apple to help the FBI access information from a cell phone used by terrorists in the San Bernardino shootings last December that left 14 dead and 22 wounded. The contents of the phone are encrypted. Attempts to crack the password would, after the 10th fail, erase all the content.

The FBI has asked Apple to create a backdoor that would prevent that from happening, but Apple CEO Tim Cook has refused, saying to do so would set a dangerous precedent, put the data security of millions of people at risk and threaten their civil liberties.

UNH Today asked James Ramsay, professor of security studies at UNH Manchester, to comment on the issue.

What is at the heart of the standoff between Apple and the FBI?

The recent relationship between Apple, Inc., and the FBI presents challenges to our concepts of law enforcement, security and privacy. The main function of homeland security is, and always has been, the defense of liberty and the protection of the free flow of people and commerce.

On one hand, Apple (and other corporations like it) has a fiduciary obligation to customers and shareholders to provide "adequate" security to prevent identity theft, financial loss, etc. If one's personal identifying information were (relatively) easy to hack, people would be less inclined to buy or use the product — a critical point, given how our society has evolved in the last 25 years.

JAMES RAMSAY, PROFESSOR OF SECURITY STUDIES, UNH MANCHESTER

This is not only a very legitimate business strategy, I would submit that it is also an incredibly necessary one to the health of our economy and, by extension, our privacy and national security. We need to appreciate how deeply entrenched and dependent we are on digital transactions. Consider that for many, payroll, healthcare and even retirement and savings are routinely done digitally and particularly on smart devices like the iPhone. This is a major reason Apple built the encryption logic as securely as they did; they want to protect the tens of millions of people using their devices from financial ruin and identity theft.

On the other hand, the FBI has a fiduciary and congressional charter to protect the U.S. population as a federal law enforcement agency. And within this role they are considered the lead U.S. agency in counterterrorism efforts.

What is to be gained from unlocking the phone?

Authorities, as well as the reasonable person, suspect that the San Bernardino terrorists quite likely have personal information and other connections or networking or data on their phones, as so many of us do today. Speedy access to this information would add depth of understanding to not only what they did but how they did it and, more importantly, who they worked with, hung out with and with whom they networked and conspired. Such data may also provide clues as to how we might prevent a similar incident from occurring.

In this case, as in all such cases, such information is central to both investigation and prevention efforts. As such, the FBI is completely legitimate in their need for such information and their request to Apple, Inc. We might consider such a request to be materially no different than getting a search warrant and going through personal belongings in one's home.

ALUMNI

UNH Today is produced for the UNH community and for friends of UNH.
The stories are written by the staff of UNH Communications and Public Affairs.
Email us: unhtoday.editor@unh.edu.

MANAGE YOUR SUBSCRIPTION **CONTACT US**

Like us on Facebook

Follow us on Twitter

Follow us on YouTube

Follow us on Instagram

Find us on LinkIn

UNH Today RSS feeds