Your on the Street Reporter

Uyless Black

FBI vs. Apple: A Fool's Mission

Opinion

COEUR d'ALENE PRESS

Editorial

What's your privacy worth?

Local writer and Internet expert Uyless Black focused this week specifically on the Apple vs. FBI argument but asked an even bigger question: What's our First Amendment-ensured privacy worth compared to our security?

While our Founding Fathers saw well out into the future, they could not have imagined the worlds that now exist behind billions of passwords. These worlds are being recreated every day through the Internet, a great tool, yes, but also a weapon with unprecedented power. Many of us are trying to figure out what access to these password-protected worlds — our most important work, our personal relationships with others, maybe even our secret forays into forbidden lands on the 'net — is worth.

A lot, you say? Well, how much? Are you unwilling to sacrifice any of your priceless privacy if that position means you risk losing it all?

In his 2015 book "Lights Out," journalist Ted Koppel shares an illustration that came from a Massachusetts lawmaker. Keep in mind that Koppel, and the Democratic lawmaker, are ardent supporters of free speech and the privacy inherent in free speech. But they are also realists when they look at the way the world is changing so dangerously, so rapidly.

In that illustration, the mother of a 13-year-old Googles for information on anorexia. Google, you understand, delivers ads customized to readers based on their searches. The mother wants Google to stop re-marketing anorexia information to a child who's already sick, and in the illustration, Google says it doesn't want rules that would inhibit its ability to gather information on every person and re-market it for profit. Yet when the government says it wants that information, not to make a profit but to protect the country, the big search engines cry foul — they don't want to release that information.

How we go forward, and where we draw the line between privacy and security, must be rigorously debated because in this new world, even our smallest enemies can forever alter the trajectory of our lives like never before.

Here's food for thought from Mr. Koppel, a good beginning in this important debate:

"If we insist too adamantly on protecting privacy, we will sacrifice both free enterprise and security. In the age of the Internet, privacy is at risk no matter what we do. What's at issue is whether we are prepared to surrender some of our privacy to our own intelligence agencies in order to protect against even greater intrusions from a growing array of external enemies. Until the general public is made to understand the scope of the actual threat, the natural inclination will be to preserve what we know and value, against what we still suspect may never happen."

COEUR d'ALENE PRESS
SERVING KOOTENAI COUNTY SINCE 1892
www.cdapress.com

Wednesday
February 24, 2016

FBI vs. Apple: A fool's mission

Part one of two: Low Hanging Fruit

The recent efforts of the FBI to force Apple to make user information inside Apple machines available to the Feds is making the headlines. Donald Trump said, "Boycott Apple until such time as they give that information." Others have made the same claims.

On Feb. 15, Judge Sheri Pym of the U.S. District Court in Los Angeles declared Apple must provide "reasonable technical assistance" to investigators seeking to unlock the data on an iPhone that had been owned by Syed Rizwan Farook, the killer in San Bernardino.

More recently, the Obama administration said Apple could retain possession and then destroy the hacking capability it would furnish the FBI. The Justice Department said, "Apple may maintain custody of the software...[or destroy it]...and make sure it does not apply to [others] without lawful court orders."

Uyless Black

Obama's effort is a fool's mission. The sophisticated terrorists, drug lords, and other high-level sociopaths have already encrypted their files within their machines. I cannot speak as an Apple user, but I can encrypt my Windows/Word files inside my Lenovo computer. I see no technical reason why any user cannot do the same with their own machine. Thus, the FBI might get inside a user's machine, such as my Lenovo personal computer, but it cannot read my encrypted files.

By writing this article, I am not giving away secrets. I use commonly available applications based on publicly known systems to make my files unbreakable.

(Truth in disclosure: Laziness takes over. I encrypt only a few of my files.) They cannot be opened by anyone who does not know the password (also called a key or passcode) to decode the material.

Once becomes Twice, then becomes Many

This one-time action of Uncle Sam requiring a computer/phone manufacturer to "open" its machine will not result in a one-time action. The next phone that is discarded near the vicinity of a terrortist act (a drug-related killing, etc.) will have the same result: Uncle Sam will demand: "Open this machine so the government can examine its contents."

If Apple writes the software to open one iPhone, it has the software to open all iPhones (on Apple's new operating system). This kind of backdoor is what Apple has sought to avoid in its new products, thus giving its customers more security.

I applaud Apple for its approach. Among other attritbutes, it marks Apple as a company that has a goal of protecting its customers' privacy, instead of the Googles of the world, who make their living exposing their customers' privacy.

It is conceivable that laws will be passed giving the government the technology to perfrom this "opening" on its own volition, yet without sufficient legal oversight. If you doubt my claim, check the recent court decrees on NSA doing illegal "wire taps" of cellular phone and Internet traffic.

Low hanging fruit

Most Interent users assume their files — letters, medical reports, et al — are known only to themselves and their communicating partners. But if we are doubtful, if we wish to keep our correspondence completely private, we can do so.

All it takes is to follow a few simple instructions, prompted by user-friendly screens (explained in a CDA Press article on Jan. 6, 2016). Once altered, the files can only be read by you and those to whom you give a key, which is not all that difficult to distribute.

But you and I are likely not encrypting our notes to our loved ones, or even sensitive business reports. We are low hanging fruit, easily picked off by governments and commercial enterprises.

This low hanging fruit may include the files on the Apple iPhone of the San Bernardino killer and other (as-of-now) clueless terrorists. Unwary killers might not know their files inside their machines can indeed be read. But many of them do know how to encrypt the traffic that is sent on public networks.

The situation brings forth the question: How much freedom do we forsake to gain more security? I cannot pretend to know the answer to this question. I can only offer some ideas about the subject in the second part of this article.

Uyless Black is an award-winning author who has written 40 books on a variety of subjects. His latest book is titled "2084 and Beyond," a work on the origins and consequences of human aggression. He resides in Coeur d'Alene.

FBI vs. Apple: A Fool's Mission

Part Two of Two: High Hanging Fruit

In the first part of this article, I described the confrontation between the U.S. Government and the Apple Company about the issue of Uncle Sam gaining access to Apple's most recent iPhone system. I explained that much of Uncle Sam's initial efforts would result in a treasure of low hanging "information fruit." For this second part, we look at the higher fruit on the tree.

High Hanging Fruit

The big-time players already know how to encrypt their files inside their machines using public software or likely in the future, software created by the terrorists themselves.

Thus, even if the government forces Apple to break into an Apple machine, the files inside that machine can be deciphered using a key known only to the owner of the machine. The Feds and hacks can examine and alter (for the hacks, damage) much of the machine's functions. But they still cannot get into the encrypted files inside the machine.

Uyless Black

This encrypted file can then be sent through the Internet.

What will Uncle Sam gain by having the ability to open anyone's machine? In the short run, information the user has not yet encrypted. In the long run, nothing except the information people don't care if anyone knows about — the low hanging fruit. But many people will encrypt their files for the sake of privacy.

There you have it, an unbreakable file. The FBI is into a suspect's machine. The FBI can scout-around its insides. But the FBI cannot decrypt the suspect's encrypted files. Thanks to American technology, ISIS is executing public encryption/decryption systems, but made secret by the Advanced Encryption Standard (AES) (Again, see "The Internet: Protecting User Content," Coeur d' Alene Press, January 6, 2016).

An ISIS killer or the dangerous hack, bent on doing harm, will learn (or already knows) how to use an encryption key for his/her files. It is cumbersome to let that key be known to a recipient, but far from infeasible. It fact, it is not all that difficult.

If the backdoors of the world's computers are allowed to be opened, a user will have no choice but to attempt to protect its contents. What a waste of time and money, with so little to gain.

In the meantime, we can be assured ISIS is already behind the door of Uncle Sam's backdoor project, busily and routinely using encryption on its files.

Oh, the FBI will protect this secret? Last week on 60 Minutes, the FBI Director admitted his computer had been hacked. So can Apple's system.

The Tip of the Security Iceberg

Less democratic countries, such as China and Iran, are hoping Apple will relent to Uncle Sam's demands and are already gearing-up to challenge Apple, Dell, Lenovo, and other manufacturers. Apple spent much time to get into markets ruled by despots. Amazingly, it was able to keep its security protocols intact. If Apple bends to Uncle Sam, it will have to bend to other governments. Simply stated, it sets a precedent. Meanwhile, the smart users will encode their files to make them impregnable.

Uncle Sam can glean a vast amount of precise and accurate information on the sociopaths of the world with Big Data and metadata operations. Uncle should be allowed unfettered access to metadata, the subject of a previous article (CDA Press, January 8, "Big Data and Metadata").

The government's backdoor program will eventually yield little information. Initially, there will be low hanging fruit from the slow learners. In the long run (and likely even now) the fruit will be inedible because it cannot be read. Some information might remain readable, but the ISISes of the world know the same tricks as America's geeks.

The current actions of the U.S. government will have major implications on Americans' civil liberties and even the way citizens go about their day-by-day Internet lives. They will now have to protect their once secure files on their machines.

I have great respect for the FBI and NSA. They are dedicated to keep us safe from some very dangerous people. Yes, they go "off track" sometimes in their zeal to do their job. But we should be glad they are in our corner.

Nonetheless, President Obama is pursuing a fool's mission with his approach to this situation. In the long run, the low hanging fruit will have been picked and the high hanging fruit will be inedible.

Meanwhile, America's adversaries' security saliva is dripping from their jowls: If Uncle Sam can force Apple and others to open their machines, so can other governments. And to read what? Ultimately, unreadable text.

Uyless Black is an award-winning author who has written 40 books on a variety of subjects. His latest book is titled "2084 and Beyond," a work on the origins and consequences of human aggression. He resides in Coeur d'Alene.