BusinessWorld ONLINE

The potential spy in your pocket

By Patrick G. Eddington

March 18, 2015

As Google's Android smartphone operating system was coming under attack in fall 2012 from malware with the colorful names of "Loozfon" and "FinFisher," the FBI's Internet Crime Complaint Center issued an alert to help defend against the threat. "Depending on the type of phone," the FBI said, "the operating system may have encryption available. This can be used to protect the user's personal data."

How times have changed.

Last fall, when Apple and Google announced they were cleaning up their operating systems to ensure that their users' information was encrypted to prevent hacking and potential data loss, FBI Director James Comey attacked both companies. He claimed the encryption would cause the users to "place themselves above the law."

The tech community fired back. "The only actions that have undermined the rule of law," Ken Gude wrote in Wired, "are the government's deceptive and secret mass-surveillance programs."

The battle resumed in February 2015. Michael Steinbach, FBI assistant director for counterterrorism, said it is "irresponsible" for companies like Google and Apple to use software that denies the FBI lawful means to intercept data.

Yet the FBI does have a lawful means to intercept it: the Foreign Intelligence Surveillance Act. Its scope was vastly expanded by Congress in the wake of the 9/11 attacks.

It's worth noting that the FBI never asked Congress to force tech companies to build "back doors" into their products immediately after the 9/11 attacks. Only after Google and Apple took steps to patch existing security vulnerabilities did the bureau suddenly express concern that terrorists might be exploiting this encryption.

In fact, the bureau has a host of legal authorities and technological capabilities at its disposal to intercept and read communications, or even to penetrate facilities or homes to implant audio and video recording devices. The larger problem confronting the FBI and the entire U.S. intelligence community is their over-reliance on electronic technical collection against terrorist targets.

The best way to disrupt any organized criminal element is to get inside of it physically. But the U.S. government's counterterrorism policies have made that next to impossible.

The FBI, for example, targets the very Arab-American and Muslim-American communities it needs to work with if it hopes to find and neutralize home-grown violent extremists, including promulgating new rules on profiling that allow for the potential mapping of Arab- or Muslim-American communities. The Justice Department's refusal to investigate the New York Police Department's mass surveillance and questionable informant-recruitment tactics among immigrants in the Arab- and Muslim-American communities has only made matters worse.

Overseas, the Cold War style of spying — relying on U.S. embassies as bases from which CIA and other U.S. government intelligence personnel operate — is increasingly difficult in the areas of the Middle East and southwest Asia undergoing often violent political change.

Steinbach testified about this before the House Homeland Security Committee earlier this month. "The concern is in Syria," he explained, "the lack of our footprint on the ground in Syria — that the databases won't have the information we need."

Notice his reference to technology "databases" rather than the importance of the human element. The U.S. intelligence community's emphasis should be on the spy on the ground who actually gathers critical information and makes any penetration of a terrorist organization possible.

This problem is true for Yemen as well, as a recent Washington Post story highlighted:

The spy agency has pulled dozens of operatives, analysts and other staffers from Yemen as part of a broader extraction of roughly 200 Americans who had been based at the embassy in Sana, officials said. Among those removed were senior officers who worked closely with Yemen's intelligence and security services to target al-Qaeda operatives and disrupt terrorism plots often aimed at the United States.

The CIA's failure to field agents under nonofficial cover, or to recruit enough reliable local informants on the ground who could communicate securely with CIA handlers outside Yemen, is symptomatic of the agency's failure to break with its reliance on embassy-based operations throughout that part of the world. Compromising encryption technology will do nothing to solve the intelligence community's human-intelligence deficit. This is a problem the agency must address if it is ever going to be successful in finding and neutralizing terrorist cells overseas.

It boils down to the fact that the FBI and the U.S. intelligence community have failed to adapt their intelligence-collection practices and operations to meet the challenges of the "new world disorder" in which we live. As former CIA officer Philip Giraldi has noted:

[I]ntelligence agencies that were created to oppose and penetrate other nation-state adversaries are not necessarily well equipped to go after terrorists, particularly when those groups are

ethnically cohesive or recruited through family and tribal vetting, and able to operate in a low-tech fashion to negate the advantages that advanced technologies provide.

The CIA has repeatedly attempted — occasionally at high cost — to penetrate militant organizations like al Qaeda and Islamic State. Nonetheless, Washington's overall counterterrorism bias in funding and manpower has been toward using the most sophisticated technology available as the key means of battling a relatively low-tech enemy.

The FBI's new anti-encryption campaign is just the latest phase in the government's attempt to deny Islamic State and related groups the ability to shield their communications. If these militant groups were traditional nation-states with their own dedicated communications channels, we'd all be cheering on the FBI's efforts. But the Internet has become the primary means for global, real-time communications for individuals, nonprofits, businesses and governments. So it should not be treated as just another intelligence target, which is certainly the FBI's and Natural Security Agency's current mindset.

Using the legislative process to force companies to make defective electronic devices with exploitable communications channels in the hope that they will catch a tiny number of potential or actual terrorists is a self-defeating strategy. If implemented, the FBI's proposal would only make all Americans more vulnerable to malicious actors online and do nothing to stop the next terrorist attack.

When the FBI sabotages the efforts of consumers and businesses to secure their data through encryption, the agency is essentially attacking the security foundations of the online world created over the past 20 years. Last year, total global online business-to-consumer sales were nearly $1.5 trillion. That figure is expected to pass $2 trillion in just a few years' time. Encryption of those transactions is vital to the long-term success of the global online marketplace.

The FBI's attack on the encryption revolution is an assault on the efforts by citizens to maintain their Fourth Amendment rights against unlawful search and seizure. Instead of fighting the modern encryption revolution, the government should be embracing it.

Patrick G. Eddington worked as a military imagery analyst at the CIA. He is policy analyst in homeland security and civil liberties at Cato Institute.