Surveillance: Your iPhone Is Stalking You

David Dittman

September 14, 2016

Though we're not as practiced as our counterparts across the Atlantic, the United States has engaged in the art of espionage since long before we had a country to call our own.

For example, Gen. George Washington, commanding the Continental Army during the American Revolutionary War, made extensive and effective use of a spy ring that operated from Long Island and was instrumental in exposing Benedict Arnold's treachery.

Not long after our federal government was constituted, however, our information-gathering efforts metastasized into outright monitoring of the domestic population – full-blown surveillance.

John Adams, the second president of the United States, signed the Alien and Sedition Acts into law in 1798 as we slid toward war with our erstwhile ally France.

The Acts, including a measure to restrict speech critical of the government, were designed to suppress opposition, particularly the Democratic-Republican Party.

Then, during the Civil War, the government, including the U.S. Army, kept watch over groups in the Old Northwest, including the Copperheads, and suppressed activities that would or could threaten the Union war effort.

Organizing the Bureau of Military Information (BMI) and expanding on work begun by the famous Allan Pinkerton was a critical step toward ensuring battlefield success for the Army of the Potomac after 1863.

As our understanding of our destiny expanded to global proportions as a result of World War I and World War II, our intelligence capabilities grew, too.

With the National Security Act of 1947, the Office of Strategic Services completed its evolution into the CIA.

Five years later, in 1952, came the National Security Agency (NSA).

Washington's spies informed on Loyalists and detailed British troop deployments using invisible ink and bespoke secret codes.

Adams' agents monitored newspapers for "seditious libel" material such as Rep. Matthew Lyon's essay in the *Vermont Journal* that, in October 1798, earned him an indictment for publishing letters with the "intent and design" to defame the government and President Adams.

The BMI used hot-air balloons, interviews with captured prisoners and well-placed agents in Confederate territory to gather order-of-battle and troop strength data.

The game-changer — the major breakthrough that took us from nascent hegemon to global empire — was the ability to collect information on a wide scale.

The exploits of "Wild" Bill Donovan's OSS during World War II went several steps further to include more sophisticated acts such as using double agents to protect Allied operations and going "behind the lines" to disrupt enemy operations via sabotage and various guerilla activities.

It was during the second half of the 20th century that counterintelligence, paramilitary operations, assassination and coup organizing became the primary stocks in trade of the American intelligence community.

We've since gone from monitoring pamphlets and commentaries published in newspapers to monitoring real-time communication, both foreign and domestic.

J. Edgar Hoover famously collected information on the rich and powerful, though mostly for his personal aggrandizement. COINTELPRO, the FBI's effort to fight domestic political dissent, took it wide.

The CIA's Operation Mockingbird used the mainstream media to disseminate information and influence the public, violating its charter.

The ability of governments and corporations to monitor your activity and "gather" information about you is only getting more sophisticated.

Nobody really knew what was going on with the NSA, though, until James Bamford's *The Puzzle Palace* came out in 1982.

Even back then, the conclusion, as Bamford titled a December 4, 1983 article for *The Washington Post Magazine*, was that "Big Brother Is Listening."

John Poindexter, who served as deputy national security adviser (1983–85) and national security adviser (1985–86) under President Ronald Reagan, kicked it up a notch with the introduction of the concept of "Total Information Awareness" (TIA) — a "Manhattan Project for Counterterrorism" — in the aftermath of the events of September 11, 2001.

Poindexter was head of the Pentagon's Information Awareness Office (IAO) when he proposed this "vast surveillance database to track terror suspects," according to the Cato Institute.

As Cato reported in January 2003, TIA would:

… according to Poindexter, "break down the stovepipes" that separate commercial and government databases, allowing OIA access to citizens' credit card purchases, travel itineraries, telephone calling records, email, medical histories, and financial information. It would give government the power to generate a comprehensive data profile on any U.S. citizen.

The U.S. Congress defunded TIA and the OIA in late 2003.

But the activities it engaged in were picked up by other government agencies.

We know this thanks to Edward Snowden.

And we know, thanks to *Motherboard*, *Boing Boing*, and *The Intercept*, that the ability of governments and corporations to monitor your activity and "gather" information about you is only getting more sophisticated.

On August 25, 2016, *Motherboard* reported the story of "a little-known Israeli surveillance vendor called NSO Group," which is "basically a cyber arms dealer."

One of its co-founders described NSO as "a complete ghost" in a 2013*Defense News* article.

As Mike Murray, vice president of research for mobile security company Lookout, told Motherboard: "We realized that we were looking at something that no one had ever seen in the wild before. Literally a click on a link to jailbreak an iPhone in one step. One of the most sophisticated pieces of cyber-espionage software we've ever seen."

NSO's Pegasus malware "basically steals all the information on your phone, it intercepts every call, it intercepts every text message, it steals all the emails, the contacts, the FaceTime calls. It also basically backdoors every communications mechanism you have on the phone.

"It steals all the information in the Gmail app, all the Facebook messages, all the Facebook information, your Facebook contacts, everything from Skype, WhatsApp, Viber, WeChat, Telegram — you name it," said Murray.

If he does nothing else well, The Man knows how to find you.

The business of selling hacking services and other super-secretive methods of gathering information to governments is growing.

NSO, for example, has pitched to the Mexican government, and the CIA is also interested.

Two weeks after *Motherboard* published its NSO story, "Someone captured and leaked a live presentation by an RCS sales tech, demonstrating his company's cyber-weapon for spying on dissidents, criminals, and whomever else the customer wanted to infect."

Boing Boing has the video here.

And Sam Biddle reported on September 12, 2016, that *The Intercept* had come in possession of instruction manuals for Harris Corp.'s Stingray surveillance device.

Stingray is the system by which the police monitor cellular communication. Richard Tynan, a technologist with Privacy International, told The Intercept that "the 'Stingray II' device can impersonate four cellular communications towers at once, monitoring up to four cellular provider networks simultaneously, and with an add-on can operate on so-called 2G, 3G, and 4G networks simultaneously."

According to Tynan, "There really isn't any place for innocent people to hide from a device such as this."

It's easy to assume that official interest is based on NSO's claim that "it can help monitor smartphones of people targeted by government agencies."

Well, we're all targets. That's a 21st-century reality. But it was an 18th-, 19th- and 20th-century reality, too.

If he does nothing else well, The Man knows how to find you.

NBNBC

Here's a company working on identifying information of a different, less threatening sort.

Baltimore-based Vivanda's goal is "to become the world's largest food-experience management platform" by developing a "food fingerprint" for every individual.

Vivanda, a spinoff from spice, seasoning, and condiment makerMcCormick & Co. Inc. (MKC), has partnered with Germany-based software giant SAP SE (SAP) and will collaborate to provide Vivanda's FlavorPrint service to SAP's consumer food and beverage customers.

Vivanda "created a new standard for the identification of the taste and texture that allows the classification of consumer taste profiles, products, dishes, recipes and beverages."

FlavorPrint is an algorithmically generated taste profile, "much like the fingerprint of a person or a UPC code of a product."

The Baltimore Sun profiled the company and its technology in August.