New American

Written by C. Mitchell Shaw on July 18, 2016

Published in the July 18, 2016 issue of the New American magazine. Vol. 32, No. 14

Government's All-access Pass to Your Privacy

The recent legal wrestling match between the FBI and Apple over encryption is not the first time the federal government has attacked the idea of private citizens using strong encryption to protect their data and communications. Throughout the months-long ordeal, which included legal battles, a public-relations war, and congressional testimony on whether Apple should be forced to help the FBI break into an iPhone used by one of the San Bernardino shooters, one thing was clear: All of the Justice Department's protestations to the contrary notwithstanding, this was about much more than whatever data may be on that one phone in this one case.

Evidence of that is found in recent attempts at federal legislation to both expand the surveillance state and essentially ban the use of encryption. While the *FBI v. Apple* case is illustrative, it is not singular and it did not happen in a vacuum.

Round One

To understand what is at stake here, it is important to look at the first round of what have been called the "Crypto Wars." In 1991, a 37-year-old software engineer named Phil Zimmermann wrote an encryption program called Pretty Good Privacy (PGP). PGP allowed anyone with a fairly modern computer and the ability to follow instructions to encrypt their e-mails in such a way that (1) the e-mail could be read only by the intended recipient, and (2) the e-mail could be digitally "signed" in such a way that the recipient could be sure it was sent by the sender and not by an imposter. He made it available for download on the Internet — which was fairly young, but quickly growing. He also published the source code of the program in old-fashioned book form and directly exported that book all over the world.

Zimmermann — and those using his new encryption standard — quickly ran into a problem. The U.S. government classified as a munition any encryption program strong enough to actually work, and banned its export. Since the Internet made it possible for anyone in the world to get their hands on a copy of the program (and also made it *impossible* to prevent them from doing so), Zimmermann soon found himself under criminal investigation by the U.S. Customs Service for alleged violations of the Arms Export Control Act.

Michael W. Lucas literally wrote the book on PGP. In the introduction to his book, *PGP & GPG: Email for the Practical Paranoid*, he explains how — by directly exporting the source code in book form — Zimmermann turned what the U.S. government had treated as a *software* issue into a *free speech* issue:

Zimmermann originally wrote PGP in boring old everyday text (or "source code"), just like that used in

any book, and used computer-based tools to convert the human-readable text into machine-readable code. This is standard practice in the computer industry. The text is not software, just as the blueprints for a car are not a car. Both the text and the blueprints are necessary prerequisites for their respective final products, however. Zimmermann took the text and had it published in book form.

Books are not considered software, even when the book contains the "source code" instructions for a machine to make software. And books are not munitions; although many books on cryptography did have export restrictions, Zimmermann could get an export permit for his book of source code. Thus, people all over the world were able to get the instructions to build their own PGP software. They promptly built the software from those instructions, and PGP quickly became a worldwide de facto standard for data encryption.

As you might guess, the US government considered this tactic merely a way to get around munitions export restrictions. Zimmermann and his supporters considered the book speech, as in "free speech," "First Amendment," and "do you really want to go there?" The government sued, and over the next three years Zimmermann and the administration went a few rounds in the courts.

Zimmermann and the federal government went back and forth in both the investigation and subsequent lawsuits. In the end, Uncle Sam realized that the courts were likely to consider the dissemination of the written code behind the software as protected speech. Rather than risk a verdict — and a precedent — that might make the export of encryption software legally acceptable in almost any case, the federal government dropped the case and relaxed the standards for exporting software used for encryption. In 1996, President Clinton issued Executive Order 13026, essentially removing encryption from the munitions list. It was hailed as the end of the Crypto Wars and privacy was declared the victor.

If only it were that simple.

Over the last 20 years, encryption has become a standard in business. You use it without even seeing it when you transfer money or log in to certain websites. (Can you even imagine signing in to your online banking without encryption to protect that transaction?) But it has not been largely adopted by the average citizen for much of anything, including e-mail. Until recently.

The Snowden "Reveal"

In May of 2013, a 29-year-old NSA data analyst shocked the world by leaking a trove of documents confirming what many had long suspected: U.S. government agencies routinely spy on everyone, including American citizens. Programs with names such as PRISM, MYSTIC, Boundless Informant, and Xkeyscore were — in direct violation of the Fourth Amendment's guarantee "against unreasonable searches and seizures" — intercepting everything from phone calls and texts to e-mails, and browsing histories and everything in between from all Americans without anything that resembled probable cause or a warrant. Within days, Edward Snowden was one of the most talked about — and most wanted — men on the planet.

In the aftermath of those revelations, the myriad of three-letter agencies promised again and again to reform, only to be found playing a shell game with the American public. Each "reform" was, in reality, merely a re-branding that allowed the surveillance of the guilty and the innocent alike to continue and grow, proving Zimmermann correct when he told GigaOM in August of 2013, "The natural flow of technology tends to move in the direction of making surveillance easier, and the ability of computers to

track us doubles every eighteen months." We are living in a golden age of surveillance and the technology is increasing.

Fortunately, technology is an equal-opportunity tool. The same type of technology used by the NSA and other agencies to strip away the privacy and liberty of Americans is available to help those same Americans defend that privacy and liberty. In fact, Snowden used software tools — including GPG (the open-source version of Zimmermann's PGP) — to communicate with journalists when he leaked all the documents showing the state of the surveillance state. The very types of technology those agencies were using to spy were used by Snowden to stay off their radar while he revealed their spying.

While the surveillance hawks have called Snowden a traitor, a criminal, and an accessory to terrorism, those who value privacy and liberty have rightly considered him a patriot. One thing is almost certain: Had there never been an Edward Snowden, there would not likely have been any increased interest in the day-to-day use of encryption for average citizens. That interest was a direct result of — a reaction to — the heavy-handed spying to which those average citizens were subjected at the hands of agents of their own government.

As more and more of the information Snowden provided to journalists was published, people began looking for ways to protect both their data and their communications from the prying eyes of both an overreaching government and nosy corporations. After all, when you are being robbed, do you really care whether the robber wears a mask or a badge? Likewise, if someone is stealing your private information, what difference does it make whether he works for the NSA, the FBI, Apple, or Google?

In a strange turn of events fueled by free market demand for encryption products, companies including Apple and Google began to offer more and better encryption. In the summer of 2014, Apple announced that — starting with iOS 8 — users' data, including that which is stored on the device such as e-mails, contacts, and photos, would be fully encrypted by default. Apple also said the encryption process would happen on the device itself and that the company would not have access to the keys, meaning that Apple would not be able to access the encrypted data. Google followed suit by making better encryption available starting with Android 5.0. As a result, millions of Americans and others around the world have the ability to use encrypted devices to protect their communications and data.

Only All Is Good Enough

The reaction from the surveillance hawks was both immediate and venomous. Within weeks of the new encryption standards for mobile devices, FBI Director James Comey told reporters at a press conference at FBI headquarters, "What concerns me about this is companies marketing something expressly to allow people to hold themselves beyond the law." Apparently, the irony of the "beyond the law" nature of warrantless, mass surveillance was lost on Comey.

Comey's remarks — while ridiculous on their face — served as the first salvo in a public-relations war designed to stigmatize encryption as something someone would use only if they have something criminal to hide. He was soon joined by other surveillance hawks who made similarly ridiculous claims. Over the following months, the rhetoric picked up steam.

John J. Escalante, who was at the time chief of detectives in Chicago, told the *Washington Post* in September 2014 that encrypted devices are the tools of the worst criminals: pedophiles. "Apple will become the phone of choice for the pedophile," he said, adding, "The average pedophile at this point is

probably thinking, I've got to get an Apple phone."

As the public-relations war waged on, it was apparent that the smear campaign was not working. By this time, more and more encrypted devices and messaging services were available, making it easier for anyone to secure their communications against digital eavesdropping.

The surveillance hawks seemed to be looking for a picture-perfect case to push for laws to force companies to undermine the encryption built into their products and services. Demands for "backdoors" into the underlying encryption became the mantra of those whose careers were tied to the surveillance state. The terrorist attacks in Paris in November 2015 looked made to order. By portraying encrypted devices and communication services as "tools of terrorists," Comey and his ilk seemed to hope they could turn public sentiment against the technology.

In the immediate wake of the attacks in Paris, Senator Dianne Feinstein (D-Calif.) — who sits on the Senate Intelligence Committee — told MSNBC, "Silicon Valley has to take a look at their products. Because if you create a product that allows evil monsters to communicate in this way, to behead children, to strike innocents, whether it's at a game in a stadium, in a small restaurant in Paris, take down an airliner — that's a big problem."

Feinstein was not alone in her demonization of encryption. CIA Director John Brennan declared that the attacks should serve as a "wake-up call" for those misrepresenting what intelligence services do to protect innocent civilians. He cited "a number of unauthorized disclosures, and a lot of handwringing over the government's role in the effort to try to uncover these terrorists" — an obvious reference to Snowden and the supposed reforms resulting from his "unauthorized disclosures."

Foreign Policy reported that Attorney General Loretta Lynch blamed encryption in the planning and execution of the attacks in Paris and elsewhere in her testimony before the House Judiciary Committee after the attacks:

Lynch said that the use of such advanced encryption technologies has hampered investigations of individuals plotting violence in the United States. Citing unspecified investigations, Lynch said that terrorist suspects have switched from traditional communications tools to ones with end-to-end encryption, which even providers can't unlock when served with court orders to do so. By using such tools, suspects ensure that officials "no longer have visibility into those discussions" about plots, Lynch said.

Senate Armed Services Committee Chairman John McCain told MSNBC that companies providing these encrypted services should be forced to provide a "backdoor," adding, "It's time we had another key that would be kept safe and only revealed by means of a court order." As if the government that has moved heaven and earth to spy on ordinary citizens could be trusted not to abuse that power. Again. McCain continued, "Recruitment and training and equipping can go on secure sites, and we cannot let that continue to happen, in all due respect to my friends in Silicon Valley."

One thing is absent from all these accusations: evidence. Aside from vague references to "unspecified investigations," the surveillance hawks offered little in the way of making their case. And so they failed to convince citizens to give up their privacy and liberty in exchange for a hollow promise of more security. Paris turned out not to be the picture-perfect case after all.

Unfortunately, another test case soon presented itself, and the enemies of privacy — who never let a

crisis go to waste — saw their opportunity. In December 2015, a married couple launched a deadly attack in San Bernardino, California, killing 14 and seriously wounding another 22. One of the shooters in that attack, Syed Farook, left behind an encrypted iPhone 5S. Investigators played a rousing game of Keystone Cops and locked themselves out of the iCloud account to which the phone was set to back up. Now, the only way to get the data from that phone was to defeat the encryption.

Without mentioning the San Bernardino attack, Senator Richard Burr (R-N.C.), chairman of the Select Committee on Intelligence, wrote an error-laden piece for the *Wall Street Journal* in which he claimed, "Encrypted devices block law enforcement from collecting evidence. Period." As if the only item in the law-enforcement toolbox is ubiquitous surveillance, and without it no evidence can be collected. He added:

Consumer information should be protected, and the development of stronger and more robust levels of encryption is necessary. Unfortunately, the protection that encryption provides law-abiding citizens is also available to criminals and terrorists. Today's messaging systems are often designed so that companies' own developers cannot gain access to encrypted content — and, alarmingly, not even when compelled by a court order. This allows criminals and terrorists, as the law enforcement community says, to "go dark" and plot with abandon.

Manhattan District Attorney Cyrus Vance, Jr. — whose famous father was President Carter's secretary of state, as well as serving under Presidents Johnson and Kennedy as deputy secretary of defense and secretary of the Army — issued a 42-page report in January 2016 claiming that encrypted devices pose "a threat to law enforcement efforts" and are "a boon to dangerous criminals." His report calls for new laws to compel companies to build backdoors into the encryption used on mobile devices so that the companies can search the devices when a warrant is issued.

Apple vs. FBI

While this new wave in the public-relations war was moving forward, the San Bernardino investigation came into play. Apple employees assisted investigators as much as they could. As Apple CEO Tim Cook explained in an open letter to customers in February 2016:

We were shocked and outraged by the deadly act of terrorism in San Bernardino last December. We mourn the loss of life and want justice for all those whose lives were affected. The FBI asked us for help in the days following the attack, and we have worked hard to support the government's efforts to solve this horrible crime. We have no sympathy for terrorists.

When the FBI has requested data that's in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal.

As the investigation proceeded, the FBI demanded that Apple do more than provide technical assistance. The agency wanted Apple to create a fake iOS update and send it to Farook's iPhone, fooling the device into accepting a software package that would allow the agents to bypass the password protecting the encryption. Apple called that what it is — a backdoor — and refused. In the open letter to customers, Cook wrote:

We have great respect for the professionals at the FBI, and we believe their intentions are good. Up to

this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone.

Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.

The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.

Apple's decision to refuse the FBI's demands was based on the basic principles that make encryption both necessary and effective. Encryption is necessary because users need to protect their data from surveillance by overreaching government agencies, data-mining by nosy companies, and theft by hackers. Encryption is effective because the keys to unlock it are kept private. The problem with backdoors is that that is just not the way cryptography works. Providing "another key" that only government can use is a farce. Any such key would inevitably be exploited by hackers and foreign governments. Experts in cryptography agree: There is simply no way for it to be "kept safe."

Cook said essentially the same thing in his open letter to customers:

Some would argue that building a backdoor for just one iPhone is a simple, clean-cut solution. But it ignores both the basics of digital security and the significance of what the government is demanding in this case.

In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.

The government suggests this tool could be used only once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable.

While "no reasonable person would find that acceptable," the FBI, the Justice Department, and Magistrate Judge Sheri Pym of the Federal District Court for the District of Central California seemed to think it made perfect sense. In their unbalanced view of security vs. liberty, the surveillance hawks always lean toward promising security, though they often fail to deliver on that promise.

So, in February Judge Pym responded to a request from the Justice Department by ordering Apple to undermine the security of millions of smartphone users in the hopes that something useful could be found on Farook's iPhone. As this writer pointed out at the time in an online article:

The iPhone at the center of the FBI's PR and legal war against Apple was not even Farook's primary mobile phone. He had a personal phone which he destroyed before he and his wife went on their ISIS-inspired killing spree. Let that sink in. Farook had two phones: a work phone and a personal phone. His employer has access to the itemized bill on his work phone which would show every number he called

and every number that called him. In fact, Verizon has given the FBI a record of all his calls and texts. He did not destroy that phone, but he did destroy his personal phone. It doesn't take The Amazing Kreskin to figure out which of those phones he was worried about investigators accessing. It is highly unlikely that anything of any value to this investigation could be found on the phone the FBI is making such a fuss over. So, why all the fuss?

The question, "Why all the fuss?" takes on even more importance when it is realized that tech experts, including Edward Snowden and John McAfee (founder of McAfee Antivirus), said repeatedly that there were hardware hacks that would have granted the FBI access to the phone without forcing Apple to create a backdoor.

Snowden responded to the FBI's claim that "Apple has the exclusive technical means" to access the data on the phone by saying, "Respectfully, that's bulls**t." He added, "There are hardware attacks that have existed since the '90's that the FBI can mount" that would give them access to the data on the phone.

Bureaucracy and Backdoors

McAfee — who had offered to decrypt the phone himself — said that backdoors are a greater danger to national security than the problems they promise to solve. As evidence he pointed to the recent breaches of government computer systems — particularly the hack of the database of the Office of Personnel Management in which millions of Americans had their personal information stolen by hackers suspected of working for the Chinese government. These hacks, McAfee said, were traced back to weaknesses in Juniper Networks hardware used by government offices. Those weaknesses in turn were traced back to the NSA installing backdoors in those systems. Our enemies found the backdoors we had built in to spy on them, and they simply turned the tables.

So considering that backdoors are a threat to national security and that the FBI could have penetrated that one phone — which was never likely to have anything of any value on it anyway — the question remains: Why all the fuss?

Because while the public-relations war focused on that *one phone* and Comey said repeatedly that it was about that *one phone*, it turns out it was never about that one phone. It was about encryption.

For all the ostensible reasons that the intelligence and law-enforcement communities give for wanting to limit the ability of ordinary citizens to encrypt their data and communications, the real reason is that those in power love power and want a monopoly on it. Government officials — who use encrypted systems for both data storage and communications — don't want private citizens to use that same technology. These are the same individuals who go about their daily lives surrounded by armed police officers, military personnel, and private security guards while decrying the evils of an armed society. This double standard is more than mere hypocrisy; it is tyranny.

Apple fought the court order and asked for its day in court. Before that, though, there was testimony before the House Judiciary Committee. Under oath, Comey admitted that he does not understand how encryption works. When asked what had been attempted before demanding that Apple create a backdoor, Comey said, "I did not ask the questions you're asking me here today. I'm not sure I even fully understand the questions."

Vance testified as well and made it clear to the committee that if the FBI were successful in its case

against Apple, he would seek to use the tool over and over again. He added that he was not alone in that hope, saying, "Law enforcement agencies at all levels, as well as crime victims' advocates and other concerned community leaders, are watching this case with great interest." In other words, the surveillance hawks needed this case to set the precedent so that they could expand it to other cases.

The day before that congressional hearing, though, a federal judge ruled in a separate, but related, case that the FBI could not force Apple to unlock the iPhone of a suspected drug dealer. That news seemed to take what wind was left out of the FBI's sails. The day before the case was to be heard, the Justice Department dropped its case, saying it had found a way into the phone and did not need to pursue the case. Sound familiar? Just as in the Zimmermann case in the 1990s, the federal government could not let a freedom-allowing precedent be set.

Once the FBI accessed the phone, it was very quietly reported that it contained no valuable information at all.

Almost as soon as the case was dropped, Feinstein introduced legislation in the Senate to require any company offering encrypted devices or services to build in a backdoor for government. After a fairly exciting start, the bill died of benign neglect. There is simply not enough support for that type of legislation. According to a report by Reuters, not even the White House would support the bill. In late May 2016, Burr and Feinstein announced that the bill was dead. They have not given up, though. Reuters reported that Burr said, "There was no timeline for the bill" and "Feinstein said she planned to talk to more tech stakeholders." Burr reportedly said, "Be patient," indicating that the pair plans to try again next year.

Following the Orlando shooting in June, a Senate bill was introduced that would have allowed the FBI to access Internet records — including browser histories and e-mail metadata — without a warrant or a court order. As of this writing, the bill has failed — by one vote — to be cleared for a full vote, but political arm-twisting is expected, and the bill may yet see the light of day. Of course, encryption would protect Americans from that snooping.

With or without the passage of legislation, Comey is not ready to throw in the towel. Reuters reported that he said there will be more litigation over encryption, which he called the "essential tradecraft" of terrorists.

So while there is a momentary lull in the battle, the Crypto Wars are far from over. Rather than breathe a deep sigh of relief as was done in the 1990s, concerned Americans need to continue fighting back. There is little doubt that this brief victory is due to the demands of ordinary, everyday Americans who refused to fall for the public-relations smear campaign against encryption. By continuing to demand more and more of the very technology that the surveillance hawks would deny them, Americans have held the hawks at bay. At least for now.

This article is an example of the exclusive content that's available only by subscribing to our print magazine.

Written by **C. Mitchell Shaw** on July 18, 2016
Published in the July 18, 2016 issue of the New American magazine. Vol. 32, No. 14