Written by **C. Mitchell Shaw** on January 11, 2018

New FBI Director Hints at Backdoors for Encryption

After a brief pause, the surveillance hawks are again demanding an end to the encryption millions of Americans use to protect their data. Newly-minted FBI Director Christopher Wray (shown) seems to be picking up right where his disgraced predecessor James Comey left off in the war against encryption, telling the attendees at the International Conference on Cyber Security on Tuesday that strong encryption is "an urgent public safety issue."

While speaking at the conference in New York, Wray said that in the fiscal year ending September 30, the FBI was unable to access more than half of the devices it attempted to access, owing to them being encrypted. He said that the number of inaccessible devices was nearly 7,800, adding that the inability to break the encryption on those devices — despite having warrants to access the data stored on them — hinders the agency's work. The annual International Conference on Cyber Security is attended by professionals working in private sector information security, FBI agents, and representatives of international law enforcement agencies.

Wray — who took over the top spot at the FBI in August after President Trump fired Comey — said, "This is an urgent public safety issue." While giving lip service to the importance of strong encryption and security, Wray said the current situation that allows individuals to protect the data on their devices with unbreakable encryption cannot be allowed to continue, adding, "We face an enormous and increasing number of cases that rely heavily, if not exclusively, on electronic evidence." He went on to say that a solution — which is "not so clear cut" as the problem — will require "significant innovation" but that he doesn't "buy the claim that it is impossible."

What Wray appears to be working his way up to — though without as much subtlety as he may think — is the creation of a "backdoor" to encryption. A backdoor is an idea that has been proposed by surveillance hawks — and rejected by privacy advocates — for years. The battle over encryption — known as the Crypto Wars — has been going on since the early 1990s. As this writer explained in an article that originally appeared in print (in our July 18, 2016 issue) and was later published online:

> 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.

In the book *PGP & GPG: Email for the Practical Paranoid*, Michael W. Lucas explains that Zimmerman — by directly exporting the source code in book form — managed to turn what the U.S. government had treated as a software issue into a free speech issue.

As the case moved through the courts, 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.

But the Crypto Wars were far from over. While encryption has been the standard in business for more than 20 years (you use it without even seeing it when you transfer money or log in to certain websites), it has not been largely adopted by the average citizen for much of anything, including e-mail. Until recently.

The upswing in the use of powerful encryption to protect data-at-rest (data stored on a device such as a computer, mobile device, external hard drive, or USB stick) and data-in-motion (data being sent from one device to another over mobile towers, the Internet, or another network) is the direct result of people reacting to what Edward Snowden revealed to the world in May 2013: U.S. government agencies routinely spy on everyone, including American citizens.

So, while Wray (and Comey before him) as well as other surveillance hawks cry and bemoan that encryption in the hands of private citizens is — in Wray's words — "an urgent public safety issue," the reality is that they hate it because it pulls the plug on huge portions of the surveillance machine. As this writer said in that previous article:

> 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.

And while Wray and other surveillance hawks make much ado of the fact that powerful encryption keeps them out of devices *even when there is a warrant*, it is important to realize that with judges issuing warrants for intrusive searches based on no more probable cause than a suspect drinking tea and shopping at a gardening store, the reality is that warrants aren't what they used to be.

Is it any wonder that people want to be able to protect their data from the prying eyes of an overreaching government? Considering that in the rising surveillance state in the wake of 9/11, the three-letter agencies that make up the surveillance army routinely violate rules put in place to protect American citizens' privacy, the courts — while feigning shock — allow those abuses to continue, many of those abuses are so widespread and large that those in charge can't even keep up with them, the

surveillance hawks keep promising reform only to continue increasing the growth of the surveillance state, the surveillance state operates secret spy hubs in major U.S. cities to make ubiquitous surveillance more practicable, and the surveillance state itself is a threat to national security — as are encryption backdoors — ubiquitous encryption seems a natural and reasonable remedy.

But — par for the course — Wray either doesn't see it that way or at least pretends not to. One thing appears certain: At least where this issue is concerned, the new boss at the FBI is the same as the old boss.

Privacy advocates should brace themselves for another round of demands for an end to powerful encryption in the hands of private citizens. Because backdoors — regardless of promises that only law enforcement could use them and then only with a warrant — are exactly that: the end of any encryption that works — which is the goal of the surveillance state.

(This article was written on this writer's System 76 Bonobo Extreme laptop running Linux and protected by LUKS encryption.)

Photo: AP Images