Encryption: Christopher Wray's "Huge, Huge Problem" is an Age-Old Inconvenience

Less than three months into his tenure as director of the Federal Bureau of Investigation, Christopher Wray wants you to know that the Trump administration's policy on encryption is business as usual: Keep trying to break it, keep pretending it's a new obstacle, keep thumping the rail and demanding unrealistic limitations on it.

In an October 22 speech to the International Associations of Chiefs of Police, Wray complained that in the first 11 months of 2017, his agents found themselves unable to access the content of more than 6,900 mobile devices.

"To put it mildly, this is a huge, huge problem," Wray complained, citing various criminal activities as hobgoblins before going on to the usual faux-reasonable claim that "there's a balance that needs to be struck between encryption and the importance of giving us the tools we need to make the public safe."

Wrong, Mr. Wray. There's no "balance" involved. Encryption is a fact of life that you're just going to have to live with. And it's been that way for a long, long time.

Theoretically unbreakable encryption has been around since at least as early as 1882 when Frank Miller invented and described the "one-time pad." A pen, a piece of paper, and a way to generate random numbers is all anyone needs to frustrate Christopher Wray's desire to read our mail.

In the Internet age, Phil Zimmerman's Pretty Good Privacy "public key" encryption framework is more than a quarter century old, still going strong, and available in various forms for most computer operating systems.

Yes, encryption can frustrate criminal investigations. Some of the Zodiac Killer's hand-encrypted messages remain unbroken more than 40 years after his killings ceased.

Whining about it won't change it. The "balance" Wray and his counterparts in other federal agencies and abroad (such as UK Home Secretary Amber Rudd) keep calling for amounts to outlawing properties of math and logic that they find inconvenient. Maybe they should do something about that pesky gravity while they're at it.

If the encryption whiners get their way on policy and legislation, they'll face two utterly predictable outcomes:

First, "the bad guys" — terrorists and criminals, real and imagined — will continue to use strong encryption. The problem with outlawing math and logic is that neither criminals nor

math and logic give a hoot about human desires masquerading as “laws.”

Second, countries where governments try to require “back doors” in encryption and other similarly stupid ideas will become losers in the race to the future. Tech companies in those countries will either go out of business or move their operations to jurisdictions where they’re allowed to serve their customers without Christopher Wray’s permission.

Government is not an immovable object. Encryption is an unstoppable force. Go away, Wray.