FBI Director: Government Must Have Access to Your Encrypted Data

The director of the FBI doesn't want you to use technology to encrypt your personal data. He said that for your safety the feds should have unrestricted access to everything you store in a cloud or a hard drive, write in an e-mail, or send in a text. Security, he says, trumps privacy. Besides, only a criminal has something to hide.

Actually, what FBI Director James Comey told the members of the Senate Judiciary Committee is that in order to stay a step ahead of the bad guys, the g-men should have access to any available technology to decode encrypted data. And that the government should be the arbiter of when decryption is necessary or not.

Comey made these statements during testimony he gave as part of a panel of "experts" called to speak at a hearing labelled "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy."

Tech specialists warn, however, that giving the FBI such access would necessarily open doors to data that could be exploited by "bad actors."

Comey isn't persuaded. "It is clear that governments across the world, including those of our closest allies, recognize the serious public safety risks if criminals can plan and undertake illegal acts without fear of detection," he told the committee.

Once again, the agents of the autocracy are demanding that Americans sacrifice individual liberty on the altar of "national security." That's nowhere made clearer than in the following question posed by Comey: "Are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime?"

But Jacob Sullum asked in a blog posted by *Reason*, "Are we comfortable with forcing technical design decisions that make sensitive information more readily available to people with ill intent, including people who happen to work for the government?"

Of course, Comey does pay passing respect to the "requirements and safeguards of the laws and the Constitution." But then again, the NSA and the dozen or so other federal agencies involved in erecting the Panopticon always find a constitutional pretext for their deprivations of freedom.

The fact is, the feds really believe (or claim to believe) that they have this power. As Comey explained, "We are not asking to expand the Government's surveillance authority, but rather we are asking to ensure that we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress has provided to us to keep America safe."

See? They don’t want to violate your most cherished civil liberties, but they have to in order to keep you safe.

The problem is that Comey doesn’t see himself, his agents, or any of the other servants of the surveillance state as being the source of our danger.

The NSA, FBI, IRS, DHS, and others cannot claim to be chasing terrorists on the one hand and yet admit to conducting dragnet surveillance of every electronic communication of every American on the other. Consider just a few examples of the attitude accelerating the growth of the surveillance state in America.

The IRS insists that its agents do not need a warrant to read “taxpayers’” e-mails.

According to documents obtained from the IRS as a result of a lawsuit filed by the American Civil Liberties Union (ACLU), the tax-collecting/data mining behemoth believes that Americans have “generally no privacy” when it comes to the information included in any electronic communication from e-mail to Facebook chats and direct messages exchanged on Twitter.

These forms of communication, they claim, are not protected by the expectation of privacy granted to other aspects of their personal lives; thus, IRS agents need not petition a judge for the right to snoop into the content of these communications.

How about more traditional forms of communication? The government has those covered (and catalogued) too.

A story in the *New York Times* published in July 2013 tells the story of Buffalo, New York, resident Leslie James Pickering. Pickering reports that in September of the previous year he noticed “something odd in his mail”: a “handwritten card, apparently delivered by mistake, with instructions for postal workers to pay special attention to the letters and packages sent to his home,” the *Times* story claims.

The card — a picture of which is included in the *Times* article — appears to read: “Show all mail to supv [supervisor] for copying prior to going out on the street.” Pickering’s name was written on the card, as well as the word “Confidential,” written in green ink. Apparently, Pickering was the unwitting target of a “longtime surveillance system” the *Times* calls “mail covers.”

It doesn’t stop there, however. While snail mail surveillance has been a tool of law enforcement for over a century, the program that targeted Pickering is called Mail Isolation Control and Tracking. As part of this surveillance tactic, the “Postal Service computers photograph the exterior of every piece of paper mail that is processed in the United States — about 160 billion pieces every year. It is not known how long the government saves the images.”

The federal government is even watching our terrestrial comings and goings. As *The New American* reported in 2013:

> The U.S. government exercises control over a massive and technologically advanced camera-based surveillance system that has the capacity to keep the urban population of this country under the watchful eye of government 24 hours a day.
>
> TrapWire is the name of this network of cameras and other surveillance tools. Unlike other elements of the central government’s cybersurveillance program, word about TrapWire was not leaked by Obama administration insiders. The details of this nearly unbelievable surveillance scheme were made public by WikiLeaks, the anti-secrecy group founded by Julian Assange.

> Exactly what is TrapWire? According to one description of the program, from the online *Russia Today*:
>
> > Former senior intelligence officials have created a detailed surveillance system more accurate than modern facial recognition technology — and have installed it across the United States under the radar of most Americans, according to e-mails hacked by Anonymous.
> >
> > Every few seconds, data picked up at surveillance points in major cities and landmarks across the United States are recorded digitally on the spot, then encrypted and instantaneously delivered to a fortified central database center at an undisclosed location to be aggregated with other intelligence.

As with so many of the federal government's unconstitutional efforts at placing each and every citizen of the United States under the never-blinking eye of those who consider themselves our caretakers, TrapWire is sold as being a necessary weapon in the War on Terror.

So, while FBI Director Comey insists that giving the government the key to decoding our encrypted data is the best way to keep us safe from alleged criminals, he ignores the fact that the known criminals in Washington, D.C. pose a far clearer and more pressing danger to our liberty than any supposed "terrorist" keeping his data securely hidden from the agents of the surveillance state.