ORANGE COUNTY
REGISTER

FBI director warns against data encryption

By CONOR FRIEDERSDORF
Oct. 21, 2014

If ever there was a time when Americans trusted corporations to secure their data, it has passed. In recent years, hackers have mounted attacks on Target, Twitter, Facebook, Google, Apple, Walmart, American Express, JP Morgan and scores of other companies with household names. Under President George W. Bush, telecommunications companies illegally participated in the warrantless wiretapping of American citizens. Under President Barack Obama, phone and Internet providers still cooperate in secret with the NSA. And websites big and small install tracking cookies on our computers that surveil and attempt to monetize our browsing.

The safe bet is to trust no one with your personal information, insofar as that is possible: to lock up, or encrypt, your data the same way you'd lock your diary or your house.

My laptop and smartphone include far more private information than the contents of my kitchen cabinets, hall closet and dresser drawers combined, so I'm pleased that Apple's latest computer and mobile device software makes it easier to encrypt my personal data.

As a result, Apple users are less vulnerable to having their information stolen by hackers and foreign governments, or breached by rogue employees at the Silicon Valley company itself. Google and its Android operating system offers similar data security to its customers.

There is, however, a critic of these security precautions.

FBI Director James B. Comey is worried that federal agents will now have a harder time seizing evidence on the computers and phones of bad guys. "The companies themselves won't be able to unlock phones, laptops, and tablets to reveal photos, documents, email, and recordings stored within," he has recently argued in television appearances. "That we would market devices that would allow someone to place themselves beyond the law troubles me. ... The notion that people have devices that with court orders, based on a showing of probable cause in a case involving kidnapping or child exploitation or terrorism, we could never open that phone?" he said. "My sense is that we've gone too far when we've gone there."

Comey is being overdramatic. Calls and texts made from phones and email sent from computers can still be recovered with a warrant. Only data stored on devices and nowhere else is unrecoverable.

He's also using strange logic. When homebuilders sell new tract houses to young couples, they turn over all the keys to the front door. They do not keep a set at their corporate headquarters in case the police come one day with a search warrant at an address that they built.

Nor do they build a secret trap door in the wall that encloses the guest bedroom in case kidnappers or terrorists ever make use of it.

Doing so would dramatically weaken the security and peace of mind of every homebuyer, the vast majority of whom are law-abiding citizens.

So it goes with phones and computers.

As Julian Sanchez, a scholar at the Cato Institute, points out, "A backdoor for law enforcement is a deliberately introduced security vulnerability: It requires a system to be designed to permit access to a user's data against the user's wishes." If I can't secure my data outright, if my encryption is so weak that Apple can break it at will, my data is inescapably also vulnerable to hackers, foreign governments, and unlawful seizures.

Plus, when corporations install strong encryption on their devices and export them, it weakens U.S. rivals. "An iPhone that Apple can't unlock when American cops come knocking for good reasons is also an iPhone they can't unlock when the Chinese government comes knocking for bad ones," Sanchez explains. "A backdoor mandate, by contrast, makes life easy for oppressive regimes by guaranteeing that consumer devices are exploitable by default ..."

There may be some cases where encryption keeps the FBI from gathering evidence on bad guys. But the benefits of locks that actually work far outweigh the costs. For nearly its entire history, the FBI carried out its mission without any evidence at all from smartphones. Even if they went dark tomorrow, the FBI would still have license plate scanners, CCTV cameras, facial recognition software, DNA evidence, retina scans and National Security Letters.

Technology has empowered the FBI far more than it has weakened it.