

FBI Announces Urgent Public Safety Issue

The inability of law enforcement authorities to access data from electronic devices due to powerful encryption is an "urgent public safety issue," FBI Director Christopher Wray said on Tuesday as he sought to renew a contentious debate over privacy and security.

The Federal Bureau of Investigation was unable to access data from nearly 7,800 devices in the fiscal year that ended Sept. 30 with technical tools despite possessing proper legal authority to pry them open, a growing figure that impacts every area of the agency's work, Wray said during a speech at a cyber security conference in New York.

The FBI has been unable to access data in more than half of the devices that it tried to unlock due to encryption, Wray added.

"This is an urgent public safety issue," Wray added, while saying that a solution is "not so clear cut."

Technology companies and many digital security experts have said that the FBI's attempts to require that devices allow investigators a way to access a criminal suspect's cellphone would harm internet security and empower malicious hackers. U.S. lawmakers, meanwhile, have expressed little interest in pursuing legislation to require companies to create products whose contents are accessible to authorities who obtain a warrant.

Wray's comments at the International Conference on Cyber Security were his most extensive yet as FBI director about the so-called Going Dark problem, which his agency and local law enforcement authorities for years have said bedevils countless investigations. Wray took over as FBI chief in August.

The FBI supports strong encryption and information security broadly, Wray said, but described the current status quo as untenable.

“We face an enormous and increasing number of cases that rely heavily, if not exclusively, on electronic evidence,” Wray told an audience of FBI agents, international law enforcement representatives and private sector cyber professionals. A solution requires “significant innovation,” Wray said, “but I just do not buy the claim that it is impossible.”

Wray’s remarks echoed those of his predecessor, James Comey, who before being fired by President Donald Trump in May frequently spoke about the dangers of unbreakable encryption.

Tech companies and many cyber security experts have said that any measure ensuring that law enforcement authorities are able to access data from encrypted products would weaken cyber security for everyone.

U.S. officials have said that default encryption settings on cellphones and other devices hinder their ability to collect evidence needed to pursue criminals.

The matter came to a head in 2016 when the Justice Department tried unsuccessfully to force Apple Inc to break into an iPhone used by a gunman during a mass shooting in San Bernardino, California.

The Trump administration at times has taken a tougher stance on the issue than former President Barack Obama’s administration. U.S. Deputy Attorney General Rod Rosenstein in October chastised technology companies for building strongly encrypted products, suggesting Silicon Valley is more willing to comply with foreign government demands for data than those made by their home country.

{eoa}