FBI, Justice Dept. take encryption concerns to Congress

July 8 2015, byEric Tucker

In this Sept. 1, 2010, file photo, then-U.S. Attorney for the Northern District of Georgia Sally Yates, speaks to reporters during a news conference at the Justice Department in Washington. Federal law enforcement officials, including Deputy Attorney General Yates, now the No. 2 official at the Justice Department, are pressing their concerns about encryption before Congress, where they will argue to senators on Wednesday, July 8, 2015, that the right to privacy is not absolute and must be weighed against public safety interests. At issue is encryption technology in phones and computers that Silicon Valley companies say offers customers' invaluable security in their communications and protection from hackers and corporate spies. But law enforcement officials say that same technology has made it harder for them, even with a warrant, to monitor and intercept messages shared by criminal suspects. (AP Photo/Manuel Balce

Ceneta, File)

Federal law enforcement officials warned Wednesday that data encryption is making it harder to hunt for pedophiles and terror suspects, telling senators that consumers' right to privacy is not absolute and must be weighed against public-safety interests.

The testimony before the Senate Judiciary Committee marked the latest front in a high-stakes dispute between the Obama administration and some of the world's most influential tech companies, placing squarely before Congress an ongoing discussion that shows no signs of an easy resolution. Senators, too, offered divided opinions.

FBI and Justice Department officials have repeatedly asserted that encryption technology built into smartphones makes it harder for them to monitor and intercept messages from criminal suspects, such as Islamic State sympathizers who communicate online and child predators who conceal pornographic images. They say it's critical that they be able to access encrypted communications during investigations, with companies maintaining the key to unlock such data.

But they face fierce opposition from Silicon Valley companies who say encryption safeguards customers' privacy rights and offers protections from hackers, corporate spies and other breaches. The companies in recent months have written to the Obama administration and used public speeches to argue for the value of strong encryption.

FBI Director James Comey, who has pressed his case repeatedly over the last year before think tanks and in other settings, sought Wednesday to defuse some of the tension surrounding the dispute. He told senators that he believed technology companies were fundamentally on the same page

as law enforcement, adding, "I am not here to fight a war."

"Encryption is a great thing. It keeps us all safe. It protects innovation," Comey said. "It protects my children. It protects my health care. It is a great thing."

But he warned that criminals were using encryption to create a safe zone from law enforcement. He said that concern was especially acute at a time when the Islamic State has been recruiting sympathizers through social media and then directing them to encrypted platforms that federal agents cannot access.

"Our job is to look at a haystack the size of this country for needles that are increasingly invisible to us because of end-to-end encryption," he said.

Deputy Attorney General Sally Yates said the Justice Department was not currently seeking a legislative fix for the issue and was instead hoping to work cooperatively with the technology companies. She expressed concern about end-to-end encryption in which only the user can access the communication. And she encouraged more companies—not the government—to retain a key that can unlock their customers' encrypted data in response to government requests and court orders.

"The current public debate about how to strike the careful balance between privacy rights and public safety has at times been a challenging and highly charged discussion," Yates told the committee. Personal privacy and Internet security, she said, "are not absolute. And they have to be balanced against the risks we face from creating warrant-proof zones of communication."

Sen. Dianne Feinstein, D-Calif., echoed Comey's concerns about

encryption, saying it allows "those who would do us enormous harm a respite from any kind with law enforcement."

But others reacted more warily to that perspective.

Sen. Al Franken said strong data security can protect not only personal privacy but also critical infrastructure and industry. He cited the huge breach at the Office of Personnel Management in which sensitive, unencrypted information was exposed.

Given that, he asked, "is there a danger, if we do this wrong, of there also being a national security risk there?"

Vermont Sen. Patrick Leahy, the panel's senior Democrat, questioned how much it would actually help to facilitate law enforcement's access to encrypted material given that "strong encryption's going to still be available from foreign powers."

Tech companies call the concerns overblown and have steadfastly promised to protect customer privacy.

In a speech last month, Apple CEO Tim Cook said the company would not waver in offering encryption tools to customers and said weakening encryption would have a "chilling effect on our First Amendment rights and undermines our country's founding principles."

In a May letter to the White House, a tech-company coalition argued that strong encryption protects against "innumerable" threats and urged the government to "reject any proposal that U.S. companies deliberately weaken the security of their products."