DOJ grows frustrated with tech firms over encryption

By David Shortell

Updated 9:02 PM ET, Tue October 10, 2017

STORY HIGHLIGHTS

- Deputy Attorney General Rod Rosenstein said technology companies enable criminals with encryption technology
- Negotiations between law enforcement and industry leaders has not been effective, he said

Washington (CNN)A top Justice Department official on Tuesday criticized technology companies that "enable criminals and terrorists" with encryption software and foreshadowed a new government approach to the issue that has increasingly frustrated law enforcement.

"When investigations of violent criminal organizations come to a halt because we cannot access a phone, lives may be lost," Deputy Attorney General Rod Rosenstein said in a speech at the US Naval Academy in Annapolis, Md.

"The approach taken in the recent past -- negotiating with technology companies and hoping that they eventually will assist law enforcement out of a sense of civic duty -- is unlikely to work," he said.

Though he did not outline future steps, Rosenstein, seemed to be taking up the mantle of a fight propelled by former FBI Director James Comey in the last administration.

Referred to at times as "going dark," the emergence of encrypted communication channels impenetrable to law enforcement even with proper warrants has proved an unsolvable issue.

Over the past year, the FBI was unable to access about 7,500 devices seized in investigations, Rosenstein said.
"Technology companies almost certainly will not develop responsible encryption if left to their own devices," Rosenstein said -- stopping short of singling out any specific companies. "Competition will fuel a mindset that leads them to produce products that are more and more impregnable. That will give criminals and terrorists more opportunities to cause harm with impunity."
Technology firms have regularly balked at calls by law enforcement to open up encrypted devices or reserve a key that a company could use to access content requested by court order as seeking "back doors" that would compromise their clients' privacy and expose them to hacking.
"It's called a back door because someone can sneak in" said Michelle Richardson, deputy director of the Freedom, Security and Technology Project at the Center for Democracy and Technology, which advocates for online civil liberties. "Even when the key sits in the company's hands, that can still happen."
The issue famously boiled over during the investigation into the 2015 San Bernardino terror attack, when Apple refused to unlock the iPhone of one of the shooters, Syed Farook.
After being rebuffed by the company in court, the FBI was able to eventually gain access to the phone after purchasing a "tool" from a private company -- a workaround Rosenstein on Tuesday called time-

consuming and not practical.
The new approach signaled by Rosenstein could include more litigation and public shaming of technology companies or a push for legislation that would compel the companies to comply.