Blogs
September 02, 2016

At various times over the last several years, the DOJ has pushed for updates to the Electronic Communications Privacy Act (ECPA) that would include greater access to encrypted information stored on electronic devices.

This week, FBI Director James Comey once again pressed for changes that would provide law enforcement with greater access to encrypted data, citing the need for an "adult conversation" so the public can understand how the current system is affecting the FBI's work. Under the ECPA, law enforcement needs a probable cause warrant to access the contents of emails and other electronic communications stored with third-party service providers that are less than 180 days old or unopened. They can obtain opened correspondence or messages older than 180 days old with just a subpoena. But significantly, if the requested data is stored in an encrypted format, the ECPA does not require the third-party service providers to provide law enforcement with data in an unencrypted format. Assistant Attorney General Leslie Caldwell, Director of the DOJ's Criminal Division, delivered a speech at a cybercrime symposium this summer in which she argued that "warrant-proof encryption" has increasingly hampered all sorts of criminal investigations, ranging from local murder cases to international cybercrimes. The problem, Caldwell said, is that even when law enforcement has obtained a valid warrant, if the data is encrypted on a device, law enforcement is often beholden to the device's manufacturer or a service provider to provide law enforcement with access to the data. She even cited examples of cases where prosecutors chose to not request evidence from technology companies when they knew the request would have resulted in a fruitless search. Caldwell pushed for a policy-based solution, arguing that "critical evidence comes from smart phones, computers, and online communications. These materials are increasingly unavailable to law enforcement as a result of some encryption technologies, even when we have a warrant to examine them. Our inability to access this data can stop our investigations and prosecutions in their tracks, which in turn poses a real threat to public safety and national security." Speaking at another cybercrime symposium earlier this week, Comey echoed Caldwell's comments, warning of the FBI's increasing inability to access data stored on electronic devices because widespread encryption built into smartphones is "making more and more of the room that we are charged to investigate dark." Standing behind Caldwell's calls for a legislative solution, Comey suggested that it is not the role of the FBI or tech companies to tell the American public how to govern itself. Instead, he plans to collect information that will assist in a legislative policy discussion next year. "We need to understand in the FBI, how this is exactly affecting our work, and then share that with folks," Comey said, while acknowledging that the American people may ultimately decide that privacy in electronic communications is more important than unblocking a potential investigative avenue for the FBI. As the DOJ continues to push for legislation that provides law enforcement with greater access to encrypted data, look for increased debate on the appropriate policy that balances the multiple interests at stake: public safety, cyber security, civil rights, and civil liberties.

Explore more in

White Collar & Investigations
Blog series

White Collar Briefly

Drawing from breaking news, ever changing government priorities, and significant judicial decisions, this blog from Perkins Coie’s White Collar and Investigations group highlights key considerations and offers practical insights aimed to guide corporate stakeholders and counselors through an evolving regulatory environment.

View the blog