THE DAILY SIGNAL

San Bernardino iPhone Privacy Fight Pushes Congress to Act on Encryption

Josh Siegel

February 29, 2016

Congress is preparing to wade into one of the trickier policy issues of modern times: when or if technology companies should have to comply with law enforcement's requests in accessing customers' private, secure information.

The leaders of Apple and the F.B.I.—the two parties warring over breaking into the iPhone of one of the San Bernardino shooters—are calling for Congress to finally provide clarity to a largely ungoverned space.

This week, a bipartisan pair of lawmakers, Rep. Michael McCaul, R-Texas, and Sen. Mark Warner, D-Va., will take the first action—sort of—when they introduce a bill that would form a commission to investigate how to deal with the challenges encryption has created for law enforcement.

This commission could set the table for actual legislation describing the circumstances in which companies must comply with the government to let it break through encryption technology to access private data in the course of terrorism and criminal cases, but experts are skeptical that that could happen during an election year.

Apple's general counsel and FBI Director James Comey will testify before the House Judiciary Committee on the encryption issue on Tuesday.

"This probably is an area for Congress to decide at this point," said Susan Hennessey, a national security fellow at the Brookings Institution and a former attorney at the National Security Agency.

"It's an issue dealing with competing core fundamental American notions about what civil liberties look like, and what we want our relations with law enforcement to look like," Hennessey told The Daily Signal. "When we run into those values' concerns, which tend to be hard to resolve, our collective understanding of how our governing system functions is that the proper way to fix that is through our elected representatives passing legislation."

The urgency for Congress to set clear policy comes after a federal court ordered Apple to help the FBI break into the iPhone used by Syed Rizwan Farook, one of the killers in the terrorist attack in San Bernardino, Calif., this past December.

Apple is contesting the ruling, arguing that if it were forced to develop software allowing it to unlock the phone, it would create a "backdoor" into devices protected by encryption, making the data vulnerable to hackers and terrorists.

Law enforcement, meanwhile, has long contended that increasingly more sophisticated encryption technology is hampering its ability to combat criminals.

In making its case to access the iPhone, the FBI used a statute from 1789, called the All Writs Act. The All Writs Act, at its most basic, gives federal judges the power to issue orders to make people do things within the limits of the law.

The FBI has obtained information from Apple through the All Writs Act in the past, but the technology company believes that the statute does not give law enforcement that power in this case.

Experts say the fact that law enforcement is depending on an outdated law in this case shows the importance of Congress creating new legislation to be used in situations dealing with modern technology.

"The reality is, we have changing technology that is changing the way in which data is secured, transmitted, and communicated, and the laws we have on the books do not clearly address how to access this information," said David Inserra, a homeland and cyber-security expert at The Heritage Foundation.

The issue of privacy and security is not new, and it has been addressed by Congress before.

As the use of wireless and digital communications grew in the 1990s, law enforcement was concerned that it would not be able to conduct authorized surveillance, such as wiretaps, for criminal investigations.

To respond to this concern, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) to allow the government to intercept electronic communications when lawfully authorized.

But that legislation governs the actions only of traditional mobile phone companies, not Internet-based communications services.

"Outside of the phone company, which is covered by CALEA, technology companies are not covered by any law requiring data retention or banning encryption," said Matt Mayer, a visiting fellow at the American Enterprise Institute and former Homeland Security official.

“Without any law on the books dealing with technology companies like Apple or Google, I think we are begging the courts to make decisions on a case-by-case basis, which always ends up in bad policy.”

Julian Sanchez, an expert on intelligence surveillance at the Cato Institute, said he thinks Congress will seek to extend the authority of CALEA.

“The two main approaches would be an extension of CALEA to apply to Internet providers and maybe device manufacturers, or freestanding legislation that has the equivalent effect of imposing an obligation of certain categories of companies to ensure law enforcement has the ability to recover plaintext [unencrypted information],” Sanchez said.

Though the experts caution it’s impossible to predict the exact language of any legislation, the leaders of the Senate Intelligence Committee, Richard Burr, R-N.C., and Dianne Feinstein, D-Calif., are expected to release a bill giving the government the power to break through encryption technology in certain cases.

Reflecting the divisiveness of the issue, Sanchez and Hennessey say they also foresee legislation from civil liberties advocates explicitly saying that no company should ever be obligated to provide this type of assistance.

“You can expect a full range of extreme shots across the belt from both sides,” Hennessey said. “But it’s anyone’s guess as to what legislation that can actually pass may ultimately look like.”

Indeed, the experts expect McCaul’s and Warner’s commission idea to be the most likely outcome during a presidential year.

Meanwhile, in the Apple case, the legal issues raised by the judge’s order could end up before the Supreme Court.

Yet even if Congress were to pass a law mandating that a company like Apple comply to orders like this one, experts predict that the high court will ultimately have to review the encryption issue in some way.

“Let’s pretend Congress passes a mandate law. Technology companies will fight that all the way to the Supreme Court,” Mayer said. “This would be the first time I can find where Congress would have mandated a private-sector entity to reduce consumer protection in a product it makes—because getting rid of encryption, or providing a backdoor, makes us vulnerable to cyber and terrorist attacks.”

“So my sense is, the courts will have to decide this anyway,” Mayer continued. “And I would rather they litigate that specific action by Congress than a 230-year-old statute.”