How Apple ended up in the government's encryption crosshairs

February 18 2016, by Brandon Bailey And Michael Liedtke

In this Wednesday, Sept. 9, 2015, file photo, Apple CEO Tim Cook discusses the new iPhone 6s and iPhone 6s Plus during the Apple event at the Bill Graham Civic Auditorium in San Francisco. Apple has spent years setting itself up as the champion of individual privacy and security, a decision that's landed it in the government's crosshairs over an iPhone allegedly used by one of the San Bernardino shooters. The high-profile case presents risks for Apple almost no matter what it does, and may spill over into the broader tech industry as well, potentially chilling cooperation with federal efforts to curb extremism. (AP Photo/Eric Risberg, File)

As the maker of trend-setting gadgets like the iPhone and iPad, Apple has changed the way people use technology in their daily lives. Now, after positioning itself as a champion of privacy, the tech giant has sparked a potentially momentous conflict with the federal government over encryption.

For months, Apple CEO Tim Cook has engaged in a sharp, public debate with government officials over his company's decision to shield the data of iPhone users with strong encryption—essentially locking up people's photos, text messages and other data so securely that even Apple can't get at it. Law-enforcement officials from FBI Director James Comey on down have complained that terrorists and criminals may use that encryption as a shield.

Then on Wednesday, Apple found itself in the government's crosshairs over an iPhone used by one of the San Bernardino mass shooters. A federal magistrate ordered Apple to produce software that would help federal investigators hack into that phone—not by breaking the encryption directly, but by disabling other security measures that prevent attempts to guess the phone's passcode.

Apple has five days to challenge that order, setting the stage for a legal clash that experts say could change the relationship between tech companies and government authorities in the U.S. and around the world.

"This is really a deep question about the power of government to redesign products that we use," said Ryan Calo, a University of Washington law professor who studies data security and privacy issues.

Many leading tech companies—Facebook, Microsoft, Twitter and Yahoo—were conspicuously silent about the dispute on Wednesday, although some trade groups issued statements endorsing Apple's position. Google CEO Sundar Pichai also voiced support for Apple in a

series of tweets late in the day. "Forcing companies to enable hacking could compromise users' privacy," Pichai wrote, adding that the case "could be a troubling precedent."

While tech companies have spoken against broad government surveillance in the past, the Obama administration has recently sought to enlist the tech industry's help in fighting terrorism. Several companies have recently heeded the administration's request for voluntary efforts aimed at countering terrorist postings on social media.

Civil liberties groups warned the fallout from the San Bernardino dispute could extend beyond Apple.

"This is asking a company to build a digital defect, a design flaw, into their products," said Nuala O'Connor of the Center for Democracy and Technology, a Washington-based group that has criticized government surveillance. In a statement, the center warned that other companies could face similar orders in the future.

Others said a government victory could encourage regimes in China and other countries to make similar requests for access to smartphone data. Apple sells millions of iPhones in China, which has become the company's second-largest market.

"This case is going to affect everyone's privacy and security around the world," said Lee Tien, a staff attorney for the Electronic Frontier Foundation, a digital rights group in San Francisco.

The case turns on an 18th-century law that the government has invoked to require private assistance with law enforcement efforts. Apple has also challenged a federal search warrant based on the same law in a Brooklyn drug case. Apple has complied with previous orders invoking that law—the All Writs Act of 1789—although it has argued the

circumstances were different.

While experts said the case will likely end up in appeals court, both sides seemed to be framing the debate for a public audience as much as for a judge.

The federal request "is very strategic on their part, to be sure" said Robert Cattanach, a former Justice Department lawyer who handles cyber-security cases for the Dorsey & Whitney law firm. He said it appeared the government took pains to ask only for limited assistance in a mass-murder case that horrified the nation.

Apple's Cook, however, declared the demand would create what amounts to a "backdoor" in Apple's encryption software. "If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data," he wrote in an open letter. Cook also pledged respect for law enforcement and outrage over the shootings.

Cook may have no choice but to mount a legal challenge, given his very public commitment to protecting customer data. He's made that position a part of Apple's marketing strategy, drawing a contrast with companies like Google and Facebook that sell advertising based on customers' online behavior.

Apple "can't be seen now as doing something that would make their products less safe," said Wendy Patrick, who lectures about business ethics at San Diego State University. "I think everyone saw this issue coming down the pike and Apple always knew it was going to push back when the moment came."

But in doing so, Apple risks alienating consumers who put a higher value on national security than privacy. A recent survey by the Pew Research

Center found 82 percent of U.S. adults deemed government surveillance of suspected terrorists to be acceptable. Apple's stance was already drawing fire Wednesday from GOP presidential candidate Donald Trump and commentators on Fox News.

Only 40 percent of the Pew respondents said it's acceptable for the government to monitor U.S. citizens, however. The survey also found nearly three-fourths of U.S. adults consider it "very important" to be in control over who can retrieve personal information about them.