The Washington Post

Tim Cook: Protecting America from itself — and protecting Apple from America

Fred Barbash and Justin Wm. Moyer

February 25, 2016

When murderers armed with semiautomatic weapons killed 14 people at a holiday party on the campus of the Inland Regional Center in San Bernardino, Calif., on Dec. 2, the nation was outraged and terrified. Though the traditional prayer vigils followed, the high body count and religious affiliation of the killers meant this would be no typical mass shooting. Republican presidential candidate Donald Trump called for a halt to Muslims entering the country — a declaration that found considerable support. The next month, President Obama issued executive orders to, as the White House put it, "make our communities safer." A climate of fear once again spread across the country.

But when the FBI asked Apple chief executive Tim Cook for help in the San Bernardino investigation — to unlock an iPhone used by one of the killers — he said no. Ordinarily, in such situations, everything is handled quietly. To the extent that companies talk, they talk through spokesmen and lawyers who usually say nothing except: "We don't comment on pending litigation."

But Cook dispensed with all of that. He went public, in his own name, and he did it personally, going on TV on Wednesday in an extended interview to explain himself. And now he's become the leader not just of America's most valuable company but also of a movement. Now, it's the United States vs. Tim Cook — and an extraordinary moment both for corporate America, the federal government and of course, for Cook, who, at this moment, is providing at least part of the answer to the question that has nagged him: "How do you follow Steve Jobs?"

Rallies have been organized in about 50 cities in protest of the FBI's demands. Organizations including the Electronic Frontier Foundation, the American Civil Liberties Union and Amnesty International have lined up in support of Cook.

"Apple is right to fight back in this case," said a statement from Sherif Elsayed-Ali, deputy director of global issues at Amnesty. "The FBI's request, which would in practice require Apple

to rewrite its operating system to weaken security protections, would set a very dangerous precedent. Such backdoors undermine everyone's security and threaten our right to privacy."

Apple CEO Tim Cook released a statement arguing against the FBI's recent order to hack into the San Bernardino shooter's iPhone 5c. (Jhaan Elker/The Washington Post)

Cook also has attracted support from libertarians, such as Julian Sanchez of the Cato Institute. Apple's resistance to the FBI order transcends the question of "whether the federal government can read one dead terrorism suspect's phone," he wrote, but forces us to ask "whether technology companies can be conscripted to undermine global trust in our computing devices. That's a staggeringly high price to pay for any investigation."

And this is just the beginning of what's bound to be an epic legal battle, perhaps at the Supreme Court, should the government press its demand. "We would be prepared to take this issue all the way," Cook said Wednesday evening. He's well armed for that, having already enlisted one of the nation's top Supreme Court litigators, Ted Olson, a former U.S. solicitor general. Olson is good, as a lawyer and as a symbol. Even Donald Trump may be wary of slapping a "soft-on-terrorists" label on a man who lost his wife on 9/11 — when Barbara Olson died aboard aboard American Airlines Flight 77 as it crashed into the Pentagon.

Cook is no longer just a CEO. "I think he's a national security hero right now," Nico Sell, co-chairman of Wickr, an encrypted messaging app, told NPR, "and more of us need to follow him."

The man who said "I don't consider myself an activist" when he reluctantlycame out as gay two years ago in Bloomberg Businessweek — a publication not known for its presence on every coffee table — is now talking about "the best of America" on national television, invoking the name of the country at least 14 times in 29 minutes.

"I think we're seeing something kind of unique," Michael Cusumano, a professor at the Massachusetts Institute of Technology, told Mic. "When the CEO of Apple speaks, people listen. I think that it is the same for Google or Microsoft or GE. But you don't find those CEOs speaking out very much. He's got a sharper edge to him than I think we thought he had."

"Cook has chosen to put himself and Apple at center stage on an issue of central importance to the technology industry, criminal justice, and society, with no assurance of where this choice will lead," wrote Geoff Colvin in Fortune magazine. "He apparently just believes it's time this issue got confronted head-on. That's leadership behavior, and whatever the outcome, it elevates Apple's status."

Cook's passion was in full display Wednesday night during an extended interview with ABC News. Yes — the Declaration of Independence was there, too.

Apple CEO Tim Cook says that complying with a court order to help the FBI break into an iPhone belonging to one of the San Bernardino shooters would "make hundreds of millions of customers vulnerable." (AP)

“This is our country,” Cook said. “This country is about life and liberty and the pursuit of happiness. It’s about freedom of expression and freedom of speech. These are core principles of America.”

He cited his support among the armed forces.

“I’ve gotten thousands of emails since this occurred and the largest single category of people are from the military,” he said. “These are men and women who fight for our freedom and our liberty. And they want us to stand up and be counted on this issue for them.” He added: “I am reading every one of them.”

Of course, to critics, there’s nothing heroic about Cook’s stand. Trump, another businessman leading a movement, called for a boycott of Apple until it cooperates with the government. New York Police Commissioner William Bratton and Manhattan District Attorney Cyrus Vance said Apple is compromising public safety.

“San Bernardino is now the most prominent, national example of how Silicon Valley’s decisions are thwarting serious criminal investigations and impeding public safety,” they said in the statement. “When Apple made the overnight switch to default device encryption in September 2014, the company clearly gave no notice or thought to the impact that decision would have on crime victims.”

FBI Director James B. Comey has personally challenged Cook’s stance. “We have awesome new technology that creates a serious tension between two values we all treasure — privacy and safety,” Comey wrote. “That tension should not be resolved by corporations that sell stuff for a living. It also should not be resolved by the FBI, which investigates for a living. It should be resolved by the American people deciding how we want to govern ourselves in a world we have never seen before.”

The Justice Department, meanwhile, accused Apple of fighting not for principle, but “for its business model and public brand marketing strategy.” In fact, prosecutors point out, the phone did not belong to Syed Rizwan Farook, who with his wife opened fire at the Inland Regional Center. It belonged to the county public health department, where he was an inspector. But to crack it, the government wants Apple to disable the feature that wipes the data on the phone clean after 10 incorrect tries at entering a password. That way, the government can try to crack the password using “brute force”–attempting tens of millions of combinations without risking deletion of the data, as the Post’s Ellen Nakashima explained.

There's no reason to think that Cook's rhetoric on San Bernardino isn't genuine. He has long been an advocate of encryption, defending his company's technology on NPR last year, before the attack in California.

In that interview, host Robert Siegel said: "If there's some text message that supposedly concerns hijacked airplanes and skyscrapers and dirty bombs, would you say, 'The government, you could have that?'"

Cook: "The government comes to us from time to time, and if they ask in a way that is correct, and has been through the courts as is required, then to the degree that we have information, we give that information. However, we design our products in such a way that privacy is designed into the product. And security is designed in. And so if you think about it … some of our most personal data is on the phone: our financial data, our health information, our conversations with our friends and family and co-workers. And so instead of us taking that data into Apple, we've kept data on the phone and it's encrypted by you. You control it."

Cook's message now is the same: A backdoor into the iPhone would be "sort of the equivalent of cancer," as he told ABC. It's just his delivery of that message that has changed.

And what's good for America, it seems, is good for Apple. Cook isn't defending encryption on a whim. Apple has sold more than 800 million iPhones and wants to sell more. Secrets are his brand. Indeed, Apple is working on new code for its iPhone software that would make it difficult for it to comply in the future with court orders like the one in the San Bernardino case.

"It's a masterful stroke of speechifying," Matthew Panzarino of TechCrunchwrote last year of Cook's public defenses of privacy. "… By taking this stance (which I do not believe to be disingenuous, their profit centers support it), Apple has put all other cloud companies in the unfortunate position of digging themselves out of a moral communications hole to prove their altruism when it comes to user data."

When the government — or governments — want Apple's user data, it makes it harder for the folks in Cupertino to do business. And when the biggest company in the country can't do business, that's bad. Maybe this is why, as Cook told ABC, he plans to meet with President Obama.

Indeed, some think the well-being of the entire U.S. tech sector may be at stake. "Remember the early days of the web, when people were afraid to enter their credit card details?" wrote James Allworth in Harvard Business Review. "It took years to get to a point where there was enough trust that buying things online was considered normal."

He added: "Already it's the case that America's European allies don't trust the U.S. with their citizens' social media data. After forcing a backdoor into Apple's phones — and who knows

which could be the next company that gets a knock on the door — what is the rest of the world going to think?”