

Apple's Cook in biggest policy challenge yet, on encryption

February 18 2016, by Rob Lever



Apple chief Tim Cook has put himself at the center of debates before on gay rights, same-sex marriage, climate change and other issues

Apple chief Tim Cook is taking on the US government on encryption, in the latest and biggest challenge for the CEO who is no stranger to corporate activism.

Cook has put himself at the center of debates before now on gay rights,

[same-sex marriage](#), climate change and other issues.

And he has been one of Silicon Valley's most outspoken advocates for encryption as a means to safeguard personal privacy and security, even if it means being branded as a supporter of bad actors.

But Apple's challenge of a court order to unlock an iPhone used by one of the San Bernardino killers opens up a new front in the long-running battle.

Cook is facing risks in the latest battle as Apple also seeks to hold its standing as one of the world's most important innovators and the most valuable company—a crown it briefly lost and regained within the past month.

"I'm just a tiny bit worried about Tim Cook drawing such a stark line in the sand with this case," said Ben Thompson, a technology consultant who briefly worked at Apple, on his Stratechery blog.

"The PR optics could not possibly be worse for Apple. It's a case of domestic terrorism with a clear cut bad guy and a warrant that no one could object to, and Apple is capable of fulfilling the request."



Google chief executive Sundar Pichai leant high-profile support to Apple's Tim Cook with a series of tweets

A California magistrate on Tuesday ordered Apple to provide "reasonable technical assistance" to the US Federal Bureau of Investigation to break into an iPhone used by one of the shooters in the deadly December rampage that killed 14 people and has been linked to supporters of the Islamic State organization.

Cook called it "an unprecedented step which threatens the security of our customers," and said the order "has implications far beyond the legal case at hand."

Battle for hearts, minds

Apple—and Cook—have drawn widespread praise from civil liberties advocates and industry leaders who claim that any weakening of encryption could be devastating for all technology products.

Google chief executive Sundar Pichai lent high-profile support to Cook with a series of tweets late Wednesday.

"We build secure products to keep your information safe and we give law enforcement access to data based on valid legal orders," he said. "But that's wholly different than requiring companies to enable hacking of customer devices & data. Could be a troubling precedent."

Alex Abdo of the American Civil Liberties Union also rallied to Apple's side, warning "If the FBI can force Apple to hack into its customers' devices, then so too can every repressive regime in the rest of the world".

But both Cook and Apple have also drawn fire from some who claim their failure to assist in the probe is damaging to national security.



Apple's challenge of a court order to unlock an iPhone used by one of the San Bernardino killers opens up a new front in the long-running battle

"Apple chose to protect a dead ISIS terrorist's privacy over the security of the American people," said Senator Tom Cotton of Arkansas, using an acronym for the Islamic State group.

"Regrettably, the position Tim Cook and Apple have taken shows that they are unwilling to compromise and that legislation is likely the only way to resolve this issue."

Pace University computer forensics professor Darren Hayes, who has worked as a consultant to law enforcement, also said Apple may be out of touch.

"I think that the public, once they become more educated about what is

happening, might change their stance about Apple," Hayes said.

Tech consultant Thompson suggested Cook could take a more pragmatic approach by cooperating "and then save the rhetorical gun powder" for a bigger request to insert a "backdoor" into the newest iPhones.

'Responsibility to lead'

But others believe Apple and Cook will prevail in the court of public opinion.

"Tim Cook is upholding values that we cherish, like liberty and freedom, particularly now when people are more suspicious about the government," said Roger Kay, an analyst and consultant with Endpoint Technologies Associates.

"From a PR perspective, I think the government is overplaying its hand."

Mark MacCarthy of the Software & Information Industry Association, which represents some 800 tech companies, said the government is taking a position which is "overbroad and unwise" and added that if it prevails, "it will ultimately affect the trustworthiness of every device where data is secured."

Kay noted that Cook has been willing take strong positions on public policy issues, more than his predecessor, the late Steve Jobs.

His high-profile stand coincides with similar efforts by some of his Silicon Valley counterparts, like Facebook's Mark Zuckerberg on education and philanthropy and others in the areas of privacy and conflict-free minerals.

"I think Tim Cook believes that he has a responsibility as the head of a

large corporation to lead in a general way," Kay said.

Cook's position does not conflict with his responsibility to shareholders, according to Kay, and may even help Apple's image.

"If the government can't get in without Apple's help, that speaks well for Apple's technology," he said.

© 2016 AFP

Citation: Apple's Cook in biggest policy challenge yet, on encryption (2016, February 18)
retrieved 10 April 2024 from

<https://phys.org/news/2016-02-apple-cook-biggest-policy-encryption.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--