From: **Fred Sainz** Sainz@apple.com
Subject: Tim Cook emails Apple employees
Date: February 22, 2016 at 3:31 AM
To: Fred Sainz Sainz@apple.com

FS

This morning, Apple CEO Tim Cook emailed Apple employees to thank them for their support and reiterate the reasons for the company's objection to the warrant. Below please find a copy of the email. In addition, the company has posted a publicly-facing Q&A which can be found at http://www.apple.com/customer-letter/answers/

Thank you.

Fred Sainz
Apple

Email to Apple employees from Apple CEO Tim Cook
Subject: Thank you for your support

Team,

Last week we asked our customers and people across the United States to join a public dialogue about important issues facing our country. In the week since that letter, I've been grateful for the thought and discussion we've heard and read, as well as the outpouring of support we've received from across America.

As individuals and as a company, we have no tolerance or sympathy for terrorists. When they commit unspeakable acts like the tragic attacks in San Bernardino, we work to help the authorities pursue justice for the victims. And that's exactly what we did.

This case is about much more than a single phone or a single investigation, so when we received the government's order we knew we had to speak out. At stake is the data security of hundreds of millions of law-abiding people, and setting a dangerous precedent that threatens everyone's civil liberties.

As you know, we use encryption to protect our customers — whose data is under siege. We work hard to improve security with every software release because the threats are becoming more frequent and more sophisticated all the time.

Some advocates of the government's order want us to roll back data protections to iOS 7, which we released in September 2013. Starting with iOS 8, we began encrypting data in a way that not even the iPhone itself can read without the user's passcode, so if it is lost or stolen, our personal data, conversations, financial and health information are far more secure. We all know that turning back the clock on that progress would be a terrible idea.

Our fellow citizens know it, too. Over the past week I've received messages from thousands of people in all 50 states, and the overwhelming majority are writing to voice their strong support. One email was from a 13-year-old app developer who thanked us for standing up for "all future generations." And a 30-year Army veteran told me, "Like my freedom, I will always consider my privacy as a treasure."

I've also heard from many of you and I am especially grateful for your support.

Many people still have questions about the case and we want to make sure they understand the facts. So today we are posting answers on apple.com/customer-letter/answers/ to provide more information on this issue. I encourage you to read them.

Apple is a uniquely American company. It does not feel right to be on the opposite side of the government in a case centering on the freedoms and liberties that government is meant to protect.

Our country has always been strongest when we come together. We feel the best way forward would be for the government to withdraw its demands under the All Writs Act and, as some in Congress have proposed, form a commission or other panel of experts on intelligence, technology and civil liberties to discuss the implications for law enforcement, national security, privacy and personal freedoms. Apple would gladly participate in such an effort.

People trust Apple to keep their data safe, and that data is an increasingly important part of everyone's lives. You do an incredible job protecting them with the features we design into our products. Thank you.

Tim

ANSWERS TO YOUR QUESTIONS ABOUT APPLE AND SECURITY
http://www.apple.com/customer-letter/answers/

****

Why is Apple objecting to the government's order?

The government asked a court to order Apple to create a unique version of iOS which would bypass security protections on the iPhone's lock

The government asked a court to order Apple to create a unique version of iOS which would bypass security protections on the iPhone's lock screen. It would also add a completely new capability so passcode tries could be entered electronically.

This has two important and dangerous implications:

First, the government would have us write an entirely new operating system for their use. They are asking Apple to remove security features and add a new ability to the operating system to attack iPhone encryption, allowing a passcode to be input electronically. This would make it easier to unlock an iPhone by "brute force," trying thousands or millions of combinations with the speed of a modern computer.

We built strong security into the iPhone because people carry so much personal information on our phones today, and there are new data breaches every week affecting individuals, companies and governments. The passcode lock and requirement for manual entry of passcode are at the heart of the safeguards we have built in to iOS. It would be wrong to intentionally weaken our products with a government-ordered backdoor. If we lose control of our data, we put both our privacy and our safety at risk.

Second, the order would set a legal precedent which expands the powers of the government and we simply don't know where that would lead us. Should the government be allowed to order us to create other capabilities for surveillance purposes, such as recording conversations or location tracking? This would set a very dangerous precedent.

Is it technically possible to do what the government has ordered?

Yes, it is certainly possible to create an entirely new operating system to undermine our security features as the government wants. But it's something we believe is too dangerous to do. The only way to guarantee such a powerful tool isn't abused and doesn't fall into the wrong hands is to never create it.

Could Apple build this operating system just once, for this iPhone, and never use it again?

The digital world is very different than the physical world. In the physical world you can destroy something and it's gone. But in the digital world, once created the technique could be used over and over again, on any number of devices.

Law enforcement agents around the country have already said they have hundreds of iPhones they want Apple to unlock if the FBI wins this case. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks. Of course Apple would do our best to protect that key, but in a world where all of our data is under constant threat, it would be relentlessly attacked by hackers and cybercriminals. As recent attacks on the IRS systems and countless other data breaches have shown, no one is immune to cyber attacks.

Again, we strongly believe the only way to guarantee such a powerful tool isn't abused and doesn't fall into the wrong hands is to never create it.

Has Apple unlocked iPhones for law enforcement in the past?

No.

We regularly receive law enforcement requests for information about our customers and their Apple devices. In fact, we have a dedicated team that responds to these requests 24/7. We also provide guidelines on our website for law enforcement agencies so they know exactly what we are able to access and what legal authority we need to see before we can help them.

For devices running the iPhone operating systems prior to iOS 8, and under a lawful court order, we have extracted data from an iPhone.

We've built progressively stronger protections into our products with each new software release, including passcode-based data encryption, because cyberattacks have only become more frequent and more sophisticated. As a result of these stronger protections which requires data encryption, we are no longer able to use the data extraction process on iPhones running iOS 8 or later.

Hackers and cybercriminals are always looking for new ways to defeat our security, which is why we keep making it stronger.

The government says your objection appears to be based on concern for your business model and marketing strategy. Is that true?

Absolutely not. Nothing could be further from the truth. This is and always has been about our customers. We feel strongly that if we were to do what the government has asked of us — to create a backdoor to our products — not only is it unlawful, but it puts the vast majority of good and law abiding citizens, who rely on iPhone to protect their most personal and important data, at risk.

Is there any other way you can help the FBI?

We have done everything that's both within our power and within the law to help in this case. As we've said, we have no sympathy for terrorists.

We provided all of the information about the phone that we possessed. In addition, we proactively offered advice on obtaining additional information. Even since the government's order was issued, we are providing additional suggestions after learning new information from the Justice Department's filings.

One of the strongest suggestions we offered was that they pair the phone to a previously joined network which would allow them to back-up the phone and get the data they are now asking for. Unfortunately, we learned that while the attacker's iPhone was in FBI custody the Apple ID password associated with the phone was changed. Changing this password meant the phone could no longer access iCloud services.

As the government has confirmed, we've handed over all the data we have, including a backup of the iPhone in question. But now they have asked us for information we simply do not have.

What should happen from here?

Our country has always been strongest when we come together. We feel the best way forward would be for the government to withdraw its demands under the All Writs Act and, as some in Congress have proposed, form a commission or other panel of experts on intelligence, technology and civil liberties to discuss the implications for law enforcement, national security, privacy and personal freedoms. Apple would gladly participate in such an effort.