1. The world today faces security threats from criminals and terrorists who threaten our shared commitment to a peaceful and productive future. Apple has a long history of cooperating with the UK government on a wide range of important issues, and in that tradition, thanks the Committee for the opportunity to share our views on this topic.

2. Apple is deeply committed to protecting public safety and shares the Government’s determination to combat terrorism and other violent crimes. Strong encryption is vital to protecting innocent people from malicious actors. While the Government has said it does not intend to weaken encryption, its representatives have made clear if, “the Secretary of State and a judicial commissioner think there is necessity and proportionality in order to be able to provide that information, those companies should be required to provide that information in the clear.”

3. The fact is to comply with the Government’s proposal, the personal data of millions of law-abiding citizens would be less secure.

Summary

4. Hundreds of millions of people depend on Apple’s products and services. Our customers trust Apple and their Apple devices with some of their most personal information — their financial data, health data, family photos, videos and messages.

5. Two things have changed in a short period of time: 1) the amount of sensitive information innocent individuals put on their devices; and 2) the sophistication and determination of malicious cyber-attackers. Governments, businesses, and individuals have all been victims, and we’ve all been surprised by the successful implementation of exploits the experts viewed as still merely theoretical.

6. Increasingly sophisticated hacking schemes and cyber-attacks have become the new normal as individuals live more of their lives on their devices and online. Without strong defense, these attacks have the potential to impose chaos, and threaten our way of life, economic stability and infrastructure.

7. We owe it to our customers to protect their personal data to the best of our ability. Increasingly stronger — not weaker — encryption is the best way to protect against these threats.

8. The bill threatens to hurt law-abiding citizens in its effort to combat the few bad actors who have a variety of ways to carry out their attacks. The creation of backdoors and intercept capabilities would weaken the protections built into Apple products and endanger all our customers. A key left under the doormat would not just be there for the good guys. The bad guys would find it too.
9. Encryption today is as ubiquitous as computing itself and we are all the better for it. There are hundreds of products that use encryption to protect user data, many of them open-source and beyond the regulation of any one government. By mandating weakened encryption in Apple products, this bill will put law-abiding citizens at risk, not the criminals, hackers and terrorists who will continue having access to encryption.

10. Some would portray this as an all-or-nothing proposition for law enforcement. Nothing could be further from the truth. Law enforcement today has access to more data — data which they can use to prevent terrorist attacks, solve crimes and help bring perpetrators to justice — than ever before in the history of our world.

11. If the UK Government forces these capabilities, there’s no assurance they will not be imposed in other places where protections are absent.

12. On the pages that follow, our submission will also take exception to the fact the bill would attempt to force non-UK companies to take actions that violate the laws of their home countries. This would immobilize substantial portions of the tech sector and spark serious international conflicts. It would also likely be the catalyst for other countries to enact similar laws, paralyzing multinational corporations under the weight of what could be dozens or hundreds of contradictory country-specific laws.

13. Finally, the bill would also force companies to expend considerable resources hacking their own systems at the Government’s direction. This mandate would require Apple to alter the design of our systems and could endanger the privacy and security of users in the UK and elsewhere.

14. We are committed to doing everything in our power to create a safer and more secure world for our customers. But it is our belief this world cannot come by sacrificing personal security.

Encryption

15. Every day, over a trillion transactions occur safely over the Internet as a result of encrypted communications. These range from online banking and credit card transactions to the exchange of healthcare records, ideas that will change the world for the better, and communications between loved ones. Governments like the United States fund sophisticated encryption technology including some of the best end-to-end encryption apps. Encryption, in short, protects people.

16. Protecting our customers and earning their trust is fundamental to our business model. At Apple, we’ve been providing customers easy ways to protect their data with strong encryption in our products and services for well over 10 years. In 2003, we launched FileVault to protect data on a user’s Mac. In 2010, with iOS 4, we began to encrypt data on iOS devices to keys derived from a user’s passcode. We launched FaceTime in 2010 and iMessage in 2011, both with end-to-end encryption. As users increasingly entrust Apple and their devices with sensitive information, we will continue to deploy strong encryption methods because we firmly believe they’re in our customers’ best interests, and ultimately
in the best interests of humanity. Our job is to constantly stay 10 steps ahead of the bad
guys.

17. Some have asserted that, given the expertise of technology companies, they should be
able to construct a system that keeps the data of nearly all users secure but still allows the
data of very few users to be read covertly when a proper warrant is served. But the
Government does not know in advance which individuals will become targets of
investigation, so the encryption system necessarily would need to be compromised for
everyone.

18. The best minds in the world cannot rewrite the laws of mathematics. Any process
that weakens the mathematical models that protect user data will by extension weaken the
protection. And recent history is littered with cases of attackers successfully implementing
exploits that nearly all experts either remained unaware of or viewed as merely theoretical.
Every day that companies hold the ability to decrypt their customers’ data is more time
criminals have to gain that ability. All the while, hacking technology grows more
sophisticated. What might have been adequate security for customers two years ago no
longer is and that’s why we’ve strengthened our encryption protections.

19. Strong encryption does not eliminate Apple’s ability to give law enforcement
metadata or other categories of data, as outlined in our Law Enforcement Guidelines. The
information Apple and other companies provide helps catch criminals and save lives. It is for
this reason that UK law enforcement still requests this data from us routinely. Information
about our assistance can be found at http://www.apple.com/privacy/government-
information-requests/

20. We believe it would be wrong to weaken security for hundreds of millions of law-
abiding customers so that it will also be weaker for the very few who pose a threat. In this
rapidly-evolving cyber-threat environment, companies should remain free to implement
strong encryption to protect customers.

Extraterritoriality

21. Apple has been established in Europe for more than 35 years. With the exception of
certain limited retail and human resources data, Apple is not established in the UK.

22. Under European data protection law, Apple Distribution International established in
Cork, Ireland and iTunes S.à.r.l. established in Luxembourg have data controller
responsibility for Apple and iTunes user personal data of users located in the EEA and
Switzerland.

23. We take this responsibility very seriously and face sanction from data protection
authorities and/or user litigation if we fail to meet those requirements. Additionally, user
content is stored in the United States, and US law controls access to that data by law
enforcement. Failure on the part of any relevant US entity to follow those requirements
gives rise to criminal and civil liability. Most relevant, Title III of the US Omnibus Crime
Control and Safe Streets Act would subject Apple to criminal sanctions for any unauthorized interception of content in transit.

24. As defined in relevant EU Telecommunications Law, Apple is not an electronic communications service provider. The Investigatory Powers Bill seeks to extend definitions in this area to an extent beyond that provided for in relevant EU law.

25. The draft bill makes explicit its reach beyond UK borders to, in effect, any service provider with a connection to UK consumers. In short, we believe this will lead to major issues for businesses and could ultimately put UK users at greater risk.

26. The first problem with asserting such extraterritorial powers is that there will remain a proportion of service providers which will never assist British law enforcement regardless of threatened sanction because they are underground or in jurisdictions unfriendly to British interests. It is to these providers that dangerous people will gravitate.

27. Even leaving that aside, the implications for companies such as Apple who do assist law enforcement will be profound. As well as complying with local law in the countries where we are established for the provision of our services, we will have to attempt to overlay compliance with UK law. On their face, those laws would not be in harmony. Further, we know that the IP bill process is being watched closely by other countries. If the UK asserts jurisdiction over Irish or American businesses, other states will too.

28. Those businesses affected will have to cope with a set of overlapping foreign and domestic laws. When these laws inevitably conflict, the businesses will be left having to arbitrate between them, knowing that in doing so they might risk sanctions. That is an unreasonable position to be placed in.

29. The Government has partly addressed this by providing a defense for businesses who cannot comply with a warrant because of local laws (although not in all parts of the bill - see below). However, once a third jurisdiction is overlaid (home country, UK and one other), the situation soon becomes very difficult for businesses to negotiate.

30. This will not just be an issue for companies like Apple: any British business with customers overseas might be faced with having to comply with a warrant from a foreign jurisdiction which poses it ethical problems, or impinges on the privacy of British consumers.

31. Clearly this situation could arise regardless of whatever legislation is passed in the UK. But Parliament will be leading the way with this bill and needs to carefully consider the precedent it sets.

**Equipment Interference**

32. We believe the UK is the first national Government to attempt to provide a legislative basis for equipment interference. Consumer trust in the public and private sectors can benefit from a more concrete understanding of the framework in which these activities can take place. However, it could at the same time be undermined by a blurring of the
boundaries of responsibilities, and the bill as it stands seems to threaten to extend responsibility for hacking from Government to the private sector.

33. It would place businesses like Apple - whose relationship with customers is in part built on a sense of trust about how data will be handled - in a very difficult position. For the consumer in, say, Germany, this might represent hacking of their data by an Irish business on behalf of the UK state under a bulk warrant - activity which the provider is not even allowed to confirm or deny. Maintaining trust in such circumstances will be extremely difficult.

34. For these reasons, we believe there is a need for much greater clarity as to how the powers in the bill will be applied, not least because, once again, the extension of the powers to overseas providers will set a precedent which, if followed by other countries, could endanger the privacy and security of users in the UK and elsewhere.

Specific Comments on Clauses

Clauses 189, 190 and 191

35. These clauses govern the Secretary of State's ability to require businesses to establish a technical capability to comply with warrants.

36. Paragraphs (1) to (5) of Clause 189 would authorize the Secretary of State to make regulations imposing specified obligations on an operator. Paragraph (4) states that those obligations could include ones “relating to the removal of electronic protection applied by a relevant operator to any communications or data” in other words, the removal of encryption.

37. As set out above, we believe there are significant risks to applying this power to encryption and to extending this power to overseas providers. We therefore do not believe the clause should be retained in its current form and certainly should not extend outside the UK.

38. However, this power could have a very profound effect on any business to whom the clauses apply, and the details are worth examining.

39. First, the oversight seems less rigorous than other parts of the bill. There is no judicial authorization of the requirements placed on businesses. There is no protection for businesses who cannot comply because of local laws.

40. Second, the system does not allow for a full weighing of the costs of compliance. While the clauses require some assessment of compliance cost, it is not clear how this would be calculated. Even if a consensus could be reached on the number of working hours and computing power needed to comply, a proper consideration would need to include the opportunity cost as other projects were put on hold, the knock-on effects for other services and the change in the customer relationship.
41. Third, because (as we explain above) any reduction in encryption in the UK will be exploited by regimes and bad actors not subject to the same privacy and civil liberties protections as UK law enforcement, the implications of a Notice under these clauses would go way beyond either the UK or the affected business. The bill at present does not require any consideration of this.

42. Fourth, there is no explicit obligation for the requirements on a business to be proportionate. Our reading of the bill is that although the Secretary of State might be required to take into account the benefits, costs and technical feasibility of the notice, and consult the Technical Advisory Board and (in the case of review) the Investigatory Powers Commissioner, it is at best implicit that she must only impose requirements that are proportionate. If there is a review, the bill requires that the Investigatory Powers Commissioner must consider whether the notice is proportionate, but the Secretary of State could still reject this advice.

43. The overall effect is a wide ranging power for the Secretary of State to demand a business remove encryption based on an insufficiently robust process and without regard to the full effects, leaving the business with no effective means of appeal.

44. Suggested amendments:

   The steps required of a business by a Notice should not include removal of electronic protection.
   These powers should not extend to overseas businesses; a conflict of laws exemption should be added.
   A notice under s189 should require judicial authorization.
   There should be clear and concise definitions for the following terms: "removal of electronic protection", "technical feasibility" and "reasonably practicable". These are key terms that should not be left in the first instance for argument in court. Parliament should define and agree what their intent is.
   The criteria by which the assessment is made by the Secretary of State should be made much more explicit.
   The Technical Advisory Board advice should be made available to the affected business, and in the case of a review under clause 191, the Interception Commissioner's advice as well.
   Before imposing any requirement under s189, the Secretary of State should consider whether the time spent in complying, cost (including opportunity cost), knock-on effects and change in customer relationships are reasonable and proportionate to the expected benefits.
   The Secretary of State should also be obliged to consider the impact of a notice on human rights, in the UK and globally.
   The Secretary of State should be required only to apply notices that are proportionate as advised by the Commissioner.
45. Paragraph (1) of Clause 188 would authorize the Secretary of State to give any telecommunications operator in the UK a national security notice directing the operator to take such steps as the Secretary of State considers necessary in the interests of national security. 188(4) precludes the powers under this clause being used as a shortcut if powers exist elsewhere in the bill.

46. While we take the strong view that this bill should not be used to demand the removal of encryption, we would not want to see that clarified only for a catch-all Clause 188 to allow the Secretary of State to demand it unilaterally.

47. Suggested amendment:

The Clause should be amended to clarify that it cannot be used to require businesses to remove electronic protection from their products or services.

Clause 31

48. This clause places a duty on an operator to comply with a warrant. Again, in line with our argument above, we continue to believe the duty should not be applied to overseas businesses, but have some more general comments on the clause.

49. Clause 31 would require a relevant operator to take all reasonably practicable steps for giving effect to a warrant. Although this is not explicit in the draft bill, our understanding of the government’s intention is that this would require us to remove end to end encryption if that was necessary to give effect to the warrant and considered proportionate. The Home Office indicated exactly this in the evidence to your committee we quoted above.

50. In other words, the bill as it stands means that whether or not the Secretary of State has served a business with a Clause189 order requiring it to remove electronic protection, a fresh warrant could be served on a business requiring them to provide data in the clear, backed up by the threat of imprisonment. This seems to represent a short cut for the Secretary of State to insist on removal of encryption - but of course compliance with a warrant in the timescale required by a criminal investigation is likely to be impossible.

51. Suggested amendments:

This Clause should not apply to overseas providers.
The Clause should be amended to make clear that ‘reasonably practicable steps’ cannot include removal of electronic protection unless dealt with separately under a Notice under Clause 189, subject to the amendments to that Clause we suggest above.
The definition of ‘reasonably practicable steps’ should be clarified as we set out above to distinguish it from ‘technical feasibility.’

Clauses 81 and 135

52. These clauses deal with targeted and bulk equipment interference warrants.
53. We are concerned about the way in which the bill could make private companies implicated in the hacking of their customers.

54. Clause 81(2) provides that a warrant can be served on a person to require them to assist in hacking.

55. Is the intention that persons receiving a warrant would knowingly let the security services break into their equipment or services or allow them to use that equipment to break into equipment used by a third party? Or does the envisaged power go even further and require persons in receipt of a warrant to actively assist in the interference of their own equipment and services?

56. These questions become even more pressing when applied to bulk equipment interference warrants. It is extremely difficult to imagine circumstances in which this could be justified, so we believe the bill must spell out in more detail the types of activities required of communications providers and the circumstances in which they are expected to carry them out. Additionally and in line with earlier comments, these clauses should not have extra-territorial effect.

57. Suggested amendments:

   The powers in this part of the bill need to be fully understood as to their intent. The bill should set out in much more detail what the requirement on a person served with a warrant will be.

   The clauses should not apply to overseas providers who would be put in an impossible conflict of laws position.

21 December 2015