

Directions: In this section, you are going to read a passage with ten statements attached to it. Each statement contains information given in one of the paragraphs. Identify the paragraph from which the information is derived. You may choose a paragraph more than once. Each paragraph is marked with a letter. Answer the questions by marking the corresponding letter on *Answer Sheet 2*.

Apple's Stance Highlights a More Confrontational Tech Industry

- A) The battle between Apple and law enforcement officials over unlocking a terrorist's smartphone is the culmination of a slow turning of the tables between the technology industry and the United States government.
- B) After revelations by the former National Security Agency contractor Edward J. Snowden in 2013 that the government both cozied up to(讨好) certain tech companies and hacked into others to gain access to private data on an enormous scale, tech giants began to recognize the United States government as a hostile actor. But if the confrontation has crystallized in this latest battle, it may already be heading toward a predictable conclusion: In the long run, the tech companies are destined to emerge victorious.
- C) It may not seem that way at the moment. On the one side, you have the United States government's mighty legal and security apparatus fighting for data of the most sympathetic sort: the secrets buried in a dead mass murderer's phone. The action stems from a federal court order issued on Tuesday requiring Apple to help the Federal Bureau of Investigation (FBI) to unlock an iPhone used by one of the two attackers who killed 14 people in San Bernardino, California, in December.
- D) In the other corner is the world's most valuable company, whose chief executive, Timothy Cook, has said he will appeal the court's order. Apple argues that it is fighting to preserve a principle that most of us who are addicted to our smartphones can defend: Weaken a single iPhone so that its contents can be viewed by the American government and you risk weakening all iPhones for any government intruder, anywhere.
- E) There will probably be months of legal confrontation, and it is not at all clear which side will prevail in court, nor in the battle for public opinion and legislative favor. Yet underlying all of this is a simple dynamic: Apple, Google, Facebook and other companies hold most of the cards in this confrontation. They have our data, and their businesses depend on the global public's collective belief that they will do everything they can to protect that data.
- F) Any crack in that front could be fatal for tech companies that must operate worldwide. If Apple is forced to open up an iPhone for an American law enforcement investigation, what is to prevent it from doing so for a request from the Russians or the Iranians? If Apple is forced to write code that lets the FBI get into the iPhone 5c used by Syed Rizwan Farook, the male attacker in the San Bernardino attack, who would be responsible if some hacker got hold of that code and broke into its other devices?
- G) Apple's stance on these issues emerged post-Snowden, when the company started putting in place a series of technologies that, by default, make use of encryption(加密) to limit access to people's data. More than that, Apple—and, in different ways, other tech companies, including Google, Facebook, Twitter and Microsoft—have made their opposition to the government's claims a point of corporate pride.

- H) Apple's emerging global brand is privacy; it has staked its corporate reputation, not to mention the investment of considerable technical and financial resources, on limiting the sort of mass surveillance that was uncovered by Mr. Snowden. So now, for many cases involving governmental intrusions into data, once-lonely privacy advocates find themselves fighting alongside the most powerful company in the world.
- I) "A comparison point is in the 1990s battles over encryption," said Kurt Opsahl, general counsel of the Electronic Frontier Foundation, a privacy watchdog group. "Then you had a few companies involved, but not one of the largest companies in the world coming out with a lengthy and impassioned post, like we saw yesterday from Timothy Cook. Its profile has really been raised."
- J) Apple and other tech companies hold another ace: the technical means to keep making their devices more and more inaccessible. Note that Apple's public opposition to the government's request is itself a hindrance to mass government intrusion. And to get at the contents of a single iPhone, the government says it needs a court order and Apple's help to write new code; in earlier versions of the iPhone, ones that were created before Apple found religion on(热衷于) privacy, the FBI might have been able to break into the device by itself.
- K) You can expect that noose(束缚) to continue to tighten. Experts said that whether or not Apple loses this specific case, measures that it could put into place in the future will almost certainly be able to further limit the government's reach.
- L) That is not to say that the outcome of the San Bernardino case is insignificant. As Apple and several security experts have argued, an order compelling Apple to write software that gives the FBI access to the iPhone in question would establish an unsettling precedent. The order essentially asks Apple to hack its own devices, and once it is in place, the precedent could be used to justify law enforcement efforts to get around encryption technologies in other investigations far removed from national security threats.
- M) Once armed with a method for gaining access to iPhones, the government could ask to use it proactively(先发制人地), before a suspected terrorist attack—leaving Apple in a bind as to whether to comply or risk an attack and suffer a public-relations nightmare. "This is a brand new move in the war against encryption," Mr. Opsahl said. "We have had plenty of debates in Congress and the media over whether the government should have a backdoor, and this is an end run(迂回战术) around that—here they come with an order to create that backdoor."
- N) Yet it is worth noting that even if Apple ultimately loses this case, it has plenty of technical means to close a backdoor over time. "If they are anywhere near worth their salt as engineers, I bet they are rethinking their threat model as we speak," said Jonathan Zdziarski, a digital expert who studies the iPhone and its vulnerabilities.
- O) One relatively simple fix, Mr. Zdziarski said, would be for Apple to modify future versions of the iPhone to require a user to enter a passcode before the phone will accept the sort of modified operating system that the FBI wants Apple to create. That way, Apple could not unilaterally introduce a code that weakens the iPhone—a user would have to consent to it.
- P) "Nothing is 100 percent hacker-proof," Mr. Zdziarski said, but he pointed out that the judge's order in this case required Apple to provide "reasonable security assistance" to unlock Mr. Farook's phone. If Apple alters the security model of future iPhones so that even its own engineers' "reasonable assistance" will not be able to crack a given device when compelled by the government, a precedent set in this case might lose its lasting force. In other words, even if the FBI wins this case, in the long run, it loses.

36. It is a popular belief that tech companies are committed to protecting their customers' private data.
37. The US government believes that its access to people's iPhones could be used to prevent terrorist attacks.
38. A federal court asked Apple to help the FBI access data in a terrorist's iPhone.
39. Privacy advocates now have Apple fighting alongside them against government access to personal data.
40. Snowden revealed that the American government had tried hard to access private data on a massive scale.
41. The FBI might have been able to access private data in earlier iPhones without Apple's help.
42. After the Snowden incident, Apple made clear its position to counter government intrusion into personal data by means of encryption.
43. According to one digital expert, no iPhone can be entirely free from hacking.
44. Timothy Cook's long web post has helped enhance Apple's image.
45. Apple's CEO has decided to appeal the federal court's order to unlock a user's iPhone.