Privacy and security
隐私与安全
Code to ruin?
解密手机?
The rights and wrongs of Apple's fight with the FBI
苹果对抗 FBI 的对与错
CITIZENS have a right to both security and privacy. The difficulties arise when these two rights are in conflict, as they now are in the battle between the world's most valuable company and its most famous law-enforcement agency. Apple has refused to comply with a court order to help the FBI unlock an iPhone used by Syed Farook, one of the terrorists involved in the San Bernardino shootings in December. The company says the government's request fundamentally compromises the privacy of its users; the feds say that Apple's defiance jeopardises the safety of Americans (see article).
公民应该享有安全和隐私的权利。然而当两者冲突的时候，问题就来了：这就是目前的情形——世界上市值最高的公司站在了赫赫有名的执法机构的对立面。苹果拒绝执行一项帮助 FBI 解锁 iPhone 的法院判决，该手机是使用者名叫 Syed Farook，是参与 12 月份圣贝纳迪诺枪击案的恐怖分子之一。公司表示政府命令从根本上违背了消费者隐私权，而联邦政府则声称，如果苹果对该项判决拒不执行会危害美国人民的安全
Some frame the stand-off in terms of the rule of law: Apple cannot pick and choose which rules it will obey, they say. That is both true and beside the point. The firm has the right to appeal against a court order; if it eventually loses the legal battle, it will have to comply. The real question is whether Apple's substantive arguments are right. That hinges on two issues.
一些人把这个僵局归因为法制：苹果不能选择性地遵守法律。这个观点没错但是并不切题。公司有权对于法院判决进行上诉，如果它在终审判决中败诉，就不得不遵守。真正的问题是，苹果这种实质性的争论是否正确。这取决于两点。
The first is whether the FBI's request sets a precedent. The law-enforcers say not. This is not an attempt to build a generic flaw in Apple's encryption, through which government can walk as needed. It is a request to unlock a specific device, akin to wiretapping a single phone line. The phone belonged to a government department, not Farook. Apple and other tech firms regularly co-operate with the authorities on criminal cases; this is no different. Yet Apple is being asked to do something new: to write a piece of software that does not currently exist in order to sidestep an iPhone feature that erases data after ten unsuccessful password attempts. Later models of the iPhone than the one Farook used are harder to compromise in this way. But if the court's ruling is upheld, it signals that companies can be compelled by the state to write new operating instructions for their devices. That breaks new ground.
第一要看 FBI 的要求是否会开先例。执法机构认为不会，这并不会在苹果的加密系统中制造一个政府可以随意进出的普遍漏洞，他们只是要求解锁一个特定装置，这就相当于搭线窃听一个特定的电话一样。这部手机属于政府部门，而不再是 Farook。苹果和其他科技公司经常会配合当局解决犯罪案件，这次也并无不同。然而这次执法机构要求苹果做的是一件前所未有的事情：写一个全新的程序去阻拦 iPhone 中“输错 10 次密码就会清除所有数据”的程序设定。在 Farook 手机之后生产的新型号 iPhone 较难用这种方法破解。但是，一旦此判决被执行，就表示政府可以强令公司改写其产品的运行指令。这会为后人打破先例。

The second issue is whether that precedent is justified. And that entails a judgment on whether security would be enhanced or weakened by Apple's compliance. In the short term, the answer is that security will be enhanced. Farook was a terrorist; his phone is the only one being unlocked; and the device might give up the identity of other malefactors. But in the longer term, things are much fuzzier.

第二要看先例是否公正。问题来了：苹果此番承诺后，安全性是增强还是减弱呢?短期而言，答案是安全性会被加强。Farook 曾是个恐怖分子，他的手机是现在唯一正被解锁的，而且可能从这台设备中发现其他罪犯的身份。但长期而言，事态越来越扑朔迷离。

Security does not just mean protecting people from terrorism, but also warding off the threat of rogue espionage agencies, cybercriminals and enemy governments. If Apple writes a new piece of software that could circumvent its password systems on one phone, that software could fall into the hands of hackers and be modified to unlock other devices. If the capability to unlock iPhones exists, so will the temptation for the authorities to use it repeatedly. And if tech firms are forced to comply with this sort of request in America, it is harder for anyone to argue against similar demands from more repressive governments, such as China's. This newspaper has long argued against cryptographic backdoors and skeleton keys on these grounds. It is possible to imagine a scenario that might override such concerns: if information is needed to avert a specific and imminent threat to many lives, for example. But in this instance, Apple's case is the stronger.

安全性不仅意味着保护人们免受恐怖主义危害，还能规避流氓间谍机构、网络罪犯与敌军政府的威胁。如果苹果写了一个新的软件，能够规避一部手机的口令系统，那么软件就能落入黑客手中，被他修改并解锁其他设备。如果有能力解锁 iPhones，那么当局也同样会反复使用此项技能。如果技术公司被迫同意美国这种请求的话，那么换作其他更具压迫性的政府，例如中国，他们若提出这般相似请求，会更难对抗。本报长期反对解密后门与基于此方面的万能钥匙。可以去想象一个这样的场景，或许能扫除这些担忧：需要获取数据信息来避免对许多人构成的一次特殊紧急威胁。但在这种情形下，苹果案例比较有说服力。

Core arguments

核心论证

This battle presages others. If the courts rule against Apple, it will work to make its devices so secure that they cannot be overridden by any updates. In that event (or, indeed, if the tech firm wins the Farook case), legislators will be tempted to mandate backdoor access via the statute book. If Tim Cook, Apple's boss, is not to hasten the outcome he wishes to avoid, he must lay out the safeguards that would have persuaded the firm to accede to the FBI's request. Tech firms are at the centre of a vital policy debate (see article). Apple has rejected the authorities' solution. Now it must propose its own.

这场对战还预示了其他方面。如果法庭判苹果败诉，它将会使它的设备安全到不会被任何更新软件推翻。倘或确实科技公司在 Farook 案例上获胜，执法人员将会选择通过成文法强制指令解密后门。如果苹果老板 Tim Cook 不打算加速实现他想规避的结果，那他必须安排好本可以说服公司同意 FBI 要求的安全措施。科技公司处于重要政策争论的中心。苹果已经拒绝官方的解决方式。现如今它必须提出自己的解决方式。