THE FLETCHER SCHOOL
TUFTS UNIVERSITY

FLETCHER READS THE NEWSPAPER

Apple Battles the FBI: Consumer Privacy vs. National Security

The Apple versus FBI phone encryption case has starkly highlighted the inherent dilemma in maintaining privacy while maximizing security. The outcome of this case could have legal and ethical ramifications for consumers and businesses for decades to come. A panel of experts at The Fletcher School engaged in a dynamic discussion on this case, the kind of a precedent it will set for future business operations, and whether Apple even has the right to challenge the FBI.

The event began with two video excerpts that summarized the two sides of the argument. The first video presented Tim Cook, CEO of Apple Inc., arguing that, while his company has been actively engaged in the past in helping the FBI extract information from phones, the particular software that the FBI wants the company to develop in this case will make its customers vulnerable and potentially infringe on their civil liberties. Next, President Barack Obama posited that an absolutist view cannot be taken on this issue. He suggested that If there is probable cause of intent, just as the FBI is allowed to search people's homes and belongings, it is entitled to search a phone as well. Furthermore, he discussed that while fundamental freedoms are guaranteed by the U.S. constitution, some constraints should be imposed to ensure that we are living in a safe and civilized society.

Professor Kevin Oye initiated the Fletcher discussion by detailing the technical nuances of the case. He explained the encryption design of the iPhone whereby each file or each piece of data in the iPhone is encrypted and protected through an encryption code that rests within the phone. This system allows files coming only from Apple to be used to upgrade the phone's software, ensures security of communication, and enables encryption of user signature. Professor Oye then outlined the design of the iPhone passcode or access code: it gives the user only 10 tries to unlock the iPhone, increases the time between each incorrect passcode entry on the phone, and can only be entered from the phone's keyboard or finger print scanner. After 10 unsuccessful passcode entry attempts, all data on the iPhone is automatically erased.

Understanding the iPhone's security design is critical to comprehending the nature of the FBI's request. This request, as Professor Oye explained, asks for the elimination of the 10 attempts maximum passcode entry feature (essentially allowing for unlimited passcode entry attempts), removal of the delay between subsequent unsuccessful passcode

entries, and the ability to remotely enter the passcode, such as through a USB. One critical nuance must be kept in mind: the FBI is not asking Apple to share this firmware or decrypt information on this phone, but rather to develop this software and apply it to the specific phone in question, which will enable FBI to bypass the phone's passcode and extract pertinent information.

The discussion then moved on to the legal implications of the case, spearheaded by **Professor Michael Glennon**. Glennon began by stating that while the FBI tries to frame this case as a 'one phone only' argument, that is in fact not the reality. In a recent press conference, the FBI Director admitted that more phones could be decoded through this tool. This issue, Glennon argued, transcends national boundaries and will be used as international precedent by repressive regimes.

Glennon urged the audience to remind themselves of the key relevant legal principles at play; specifically, that "no governmental actor may act without a source of authority." Authority in this case refers to either the U.S. Constitution or a statute; it cannot and should not simply be a judge deciding the matter. Tim Cook reiterated the point that currently there is no statute that forces Apple to break into its own product and therefore it is not obligated to comply with the wishes of the FBI. The only seemingly relevant statute that perhaps can be attributed to this case is the Communications Assistance for Law Enforcement Act (CALEA) enacted in 1994 that requires phone companies to assist the FBI in setting up wire taps. However, this statute is restricted to phone companies only, and while an amendment was introduced to expand its authority in the past, it was rejected by Congress. The FBI has indicated that it will use the 1789 Al Ritz act in the absence of another statute, however it is unprecedented to seek this kind of authority under this act.

Glennon summarized by stating that the ultimate issue here is not just that of security versus privacy. It is about the meaning of the rule of law and whether judges can act as legislators, using their own authority, which has not been given to them by Congress. The key to reaching a solution in this case will require a delicate balance of one set of security interests against another.

The debate intensified when **Dean Jim Stavridis** took the position in favor of the U.S. government. Stavridis argued that this case is not one of security versus privacy, but rather about figuring out how to do both simultaneously. Regarding the question of the government's authority to compel a company to action, he pointed out that the government regularly compels private companies to do things in the name of public interest, whether it is designing military equipment or making medicines, and he believes this case is no different than these examples. He did feel that one key question we should be asking is why the FBI is targeting Apple, as this indicates that the U.S. government is unable to extract data from this iPhone on its own.

Glennon did not share Stavridis' trust in the country's security apparatus, nor his faith in its judges.. Glennon concluded by stating that the proposition that the FBI should be able to break into anyone's phone at any time is nothing less than absolutism, something the President himself urged against for this specific case.

The panel then gave the audience an opportunity to formulate and present a case to either Apple or the FBI to convince them of the other side's view. Fletcher students unanimously sought to convince Obama on changing his stance. The salient features of their arguments were:

1. Code is a form of speech and in compelling Apple to write this specific code, the FBI is infringing on the company's fundamental freedom of speech and forcing it to speak against its beliefs.
2. There is no statute that can be applied directly to this case and in giving a ruling against Apple, the court will infringe on Congress' stronghold.

Ayesha Waqar, MIB 2016
March 14, 2016