International Center for Enterprise Preparedness (InterCEP)

Apple vs. the FBI: The Inevitable Clash and its Global Ramifications

Web Forum

On November 15, 2016, **Karen J. Greenberg**, Director of the Center on National Security at Fordham University, and a noted expert on national security, terrorism, and civil liberties, led a discussion about privacy and security titled *Apple vs. the FBI: The Inevitable Clash and its Global Ramifications*. The discussion addressed recent cases of disagreement between private U.S. technology companies and government agencies with regard to customer data and privacy. The web forum discussion is summarized below.

Tensions over Private Customer Data

Business and government relations in the area of privacy and security are currently tense and in the next few years coordination between the private and public sectors could change in important ways. An important issue is the current gap in legislation in this area which needs to be addressed, not just in the courts, but also in new legislation. Improvements in the legal framework for addressing conflicts between privacy and security could ease tensions between the U.S. intelligence agencies and Silicon Valley.

The recent case with Apple in the aftermath of the December 2, 2015, San Bernardino terrorist attack highlights these tensions. When it was portrayed in the news it seemed like an interesting issue. The FBI mentioned that encryption policy needed to change because from their perspective the country could be compromised in terms of identifying terrorists and learning who they communicate with. This is liberty and security writ large. After the San Bernardino attack, the FBI needed to find out who the perpetrators were in touch with and whether there were foreign connections. The FBI assumed that the American public would be supportive of this argument but they were not.

Recent Cases of Privacy versus Security

In 2008, a classified court, a secret court, heard a case in which Yahoo was asked to turn over material the government wanted. Yahoo refused to turn over the data. The government demanded that Yahoo complied with their request. The court sided with the government and Yahoo still said no. The main reason for Yahoo's refusal was that handing over the data had the potential to create a sense of insecurity across the industry and that this kind of action was against the constitution. They also feared that people would back out of Yahoo if they believed they were being monitored. Yahoo received a daily fine of $250,000.

The discussion in court was whether the Yahoo case was a 4th amendment issue, a constitutional issue. The judges decided to rule against Yahoo by arguing that the company had indicated that the government was not acting in good faith. The court assumed that distrust is not adequate as an argument when dealing with elected officials. This court of distinguished judges said you have to trust that government officials are going to do the right thing.

On December 2, 2015, 14 people were killed and 25 were injured in San Bernardino. The perpetrators were killed and their phone became particularly important. What information could they find on that phone? Were they self-starters? The government went to Apple and asked them to disable the encryption system that was not allowing them to access what was in the phone. And Apple refused, arguing that such action would set a precedent that would compromise the security of the whole business.

Facebook, Google and Twitter agreed with Apple because this debate had been going for a long time. Technology companies understood what the risks were in terms of constitutional guarantees, philosophical concerns, and the bottom line.

What is new with these recent cases is the understanding that there are overlapping civil liberties, business and consumer interests and concerns. This means there is tremendous power behind the privacy argument.

The government relied on an act of 1789 to make their argument. The government kept requesting the information and Apple essentially never complied with the government. The lawyer representing Apple argued that the Justice Department was rolling back measures to protect financial records, credit card data, information about children, etc. This information includes details about a person's daily life. If a company were to comply with what the government was asking for then the way of life we've come to rely on would be changed/compromised.

Eventually the government found a way into the phone anyway.

Microsoft has two cases. In one, the government issued a search warrant for a server in Ireland that had data they wanted. The Electronic Communications Privacy Act will be on the forefront of these cases going forward. Microsoft appealed arguing that the government would have to go to the Irish government to make the request. The circuit court looked at the documents, thought about the law, and ruled in favor of Microsoft.

A recurring theme is that the legislation is old and inadequate. It was formulated when there was no cloud, and now we are dealing with a different sense of where people store data. One of the judges in the Microsoft case wrote that the courts have a role to protect privacy.

The second Microsoft case involves a gag order that prevents the company from revealing to certain customers that the government is asking for their data. There is no resolution so far in this case.

One of the issues that stymied privacy issues in the past is who searches for the material and in what way. For instance, if you search through Yahoo communications and emails is that different from a machine conducting the search? Is there a difference in terms of privacy whether a machine or a person is doing the search?

When President-elect Trump was asked about these cases, his response was that Apple needed to turn over information right away. What are the mechanisms in place that could force the company to turn over the information? Again, there is a tense relationship between business and government.

Although some Silicon Valley companies might consider moving outside the United States to avoid the conflict between business and government, that would be extremely difficult to do. Moreover, it would ramp up the conflict to another level.

Q&A

Can the Apple team make arguments that have not been utilized yet?

That's a really good question. The only argument they could make that they have not made is not a legal argument. They have not included their understanding of national security. They could weigh in on national security and privacy.

What impact could the election results have on privacy versus security concerns?

President-elect Trump is a business man but he is also thinking that the government is as powerful as can be. How authoritarian will he be? We may be in uncharted territory. The more interesting question is how the intelligence community is reacting to this. The intelligence community has come to terms with the fact that privacy and security are fundamental issues to this country. Respect for the constitution is deeply seated in many parts of the government. There will probably be a more heated battle, about the power of the Executive and the President, and this all depends on the appointments of director of the CIA and the other top national security appointments.

With the Republican Party controlling the Senate, the House, and the Executive branch, will there be serious legislative proposals?

What will come out of this Congress? Will there be Sunset clauses? There may be a battle because these companies are very powerful and it's different when you have strong players.

Are there any impacts on the financial sector?

Foreign policy is more likely to have more significant ramifications. How much of these financial records are vulnerable to foreign attackers? What is the legislation in terms of insurance and compliance, and how much will financial companies have to do to protect information?

Is encryption bullet proof?

How long does your shield work for? Thinking encryption will work can be a problem, it may only work for a limited time.

What happens to employees that are let go when a company has a phone policy that allows employees to use them for both personal and business purposes? Does the company have the right to erase the phone remotely, etc.?

That issue has to be discussed at the beginning, when a person is hired, and a company most likely will not be able to spring that on an employee when they leave.

What about the international arena?

The US has mentioned that it wants its own rules in this area. There has been a sense that you can do things internationally that you can't do domestically. Which government shares information with other governments? Can corporations move to other countries where they can do what they want without the need for doing what the U.S. government wants? These are issues that are likely to be increasingly discussed in the near future.

Will these cases rise to the U.S. Supreme Court?

A case may well rise to the Supreme Court, which has so far stayed away from surveillance cases, from collection of information cases. More and more courts are weighing in, but not on constitutional questions yet. At this point it is unclear where the Supreme Court stands on these issues.

Any closing remarks or take away comments?

There is currently a very interesting situation of 14 years of learning, of being aware of government surveillance of the Internet. There are many who believe the 4th amendment of the Constitution has been compromised by many government programs.

Multinational corporations seems to side with citizens, but there may be a future where citizens don't trust the government but where the multinational corporations also don't have the trust of citizens

because information might be misused. There may be a future where citizens may not feel they have control over things, where citizens will be left wondering where they can go for protection. This is an extremely delicate moment for all three of these groups and we have no idea where to go, but multinational corporations have a huge burden right now because they are extremely powerful and they can defend the bottom line and citizen interests.

Additional Resources:

- Center on National Security at Fordham University: http://www.centeronnationalsecurity.org/
- Pew Research Center - Online Privacy and Safety: http://www.pewresearch.org/topics/privacy-and-safety/
- New York University - Center for Cybersecurity: http://cyber.nyu.edu/
- New York University - Privacy Research Group: http://www.law.nyu.edu/centers/ili/privacy_research_group
- Princeton University – Security and Privacy Research Group: https://security.cs.princeton.edu/