NYU CENTER FOR CYBER SECURITY – CYBER DIALOGUES TECHNOLOGY, RISK AND GOVERNANCE

One of the objectives of this seminar was to put forward a point that cybersecurity is a field that is not only related to the technical side of things but also involves factors such as law and policy. As a student doing my graduate studies in cybersecurity I often come across the legal aspects of cybersecurity and how policies play a very important role. It is important to know and consider all these aspects to move forward in this field. I didn't realize the talk was going to be in the form of an interview. It was better being kept like this than the normal presentation type of talks. It was more like having a conversation with the audience. We had three interview sessions. All three interviews gave some very insightful views.

Ted Schlein, General Partner, Kleiner Perkins Caufield & Byers, said that security in the previous years was more concentrated towards prevention and security in recent years is more inclined towards detection and then prevention. I agree with what he said. The field of security has grown exponentially. In the current era people are more interested in finding new ways to compromise information than trying to strengthen the security of the system. But the fact is that we can only strengthen something if we know what it lacks or what all weaknesses it possesses. The second interview with Matthew Olsen, President, Consulting, IronNet Cybersecurity; Former Director, National Counterterrorism Center, was another interesting one. They covered the role of the government mostly during this talk. The Apple and FBI case was brought up where he said that this issue could not be resolved by fighting over it for two years and that all the people involved in this should gather up in a room and discuss it properly. He also said that the policy makers will play a main role in coming up with a solution. There was also some talk about how much the government can support private companies in terms of security.

The most interesting talk for me was the one with the chief of security at Facebook, Alex Stamos. He touched up on this Apple issue as well. He also strongly stated that Facebook supports Apple on this. I feel the same. People want to feel that all their personal information and belongings are safe and secure. That is why we install security systems everywhere from our homes to most of the products we buy. The present era is one such that no one can live without their phone. People rely on their mobile phones for everything from reminders to even for calculators. People store so many things in their phone like photos, secret chats, and other private information. Therefore, there is a need to let people know that whatever they have in their phones is going to stay in their phones. Asking to compromise security by placing a backdoor on the apple IPhone is not the right choice according to me. Also during the talks people had also kept asking a question, how much can we trust the government? There was also a nice car analogy made. Judith stated that car manufacturers thought of what could happen to the users and decided to place seatbelts for their protection. Alex followed this up and stated that the old approach of finding vulnerabilities and then patching them should be changed to look at how users are affected and how we can improve the security for their sake. Looking at security through the user perspective was an interesting point. These were the highlights of the talk according to me. Overall I learned a lot from these talks and look forward to attending more such seminars.