6th Committee - Legal

EGMUN 2015

Marcus Engvall - Main Chair

The question of right to privacy with regard to digital and cyber surveillance on civilians

With the rise in prominence that the Internet has experienced the past decade, certain issues that previously weren't particularly noteworthy have become important to millions of internet users worldwide. One of these hotly debated topics is the right to privacy online, which is what this topic primarily concerns itself with.

The Internet is in its very foundation a medium of information exchange, and the easier it is to transmit information the more information we choose to transmit. The widespread usage of social media is one manifestation of that. We have a tendency to share even the most intimate aspects of our life online with family and friends, but not only do we publicly share information we also privately send messages to people through protocols like email and text messaging. Most of the world's communication is handled through **digital mediums** like the Internet, and the result is a large and growing repository of information that can reveal virtually every part of a person's and group's life and activities. The keywords we use to search on search engines, the likes we hand out on social media, and the comments we post on discussion forums can form a highly accurate picture of our personal profile and indeed the profile of others. Our interconnected **social graph** is perhaps one of the most important identities we have, and as such it's not unnatural that it's fiercely defended by privacy advocates.

Indeed, the importance of our online presence is not important to only individuals, but also the **intelligence community**. International adversaries use online mediums to communicate with each other, and this treasure trove of information is thus highly useful for intelligence agencies to map out potential attacks towards their respective nations and other potential targets. The field of intelligence that deals with tracking and listening to communications is called **signals intelligence (SIGINT)**. Major players within the field of signals intelligence include the **National Security Agency (NSA)** in the United States, the **Government Communications Headquarters (GCHQ)** in the United Kingdom, and several other smaller players in other countries (including the **Försvarets Radioanstalt (FRA)** in Sweden).

Signals intelligence has a long history, and has been used for legitimate purposes in the past. However, concerns have been raised recently if their ability to monitor the global communications network is far too over-reaching or otherwise inappropriate. The criticism towards this mass-surveillance has mostly been triggered by the release of several hundred thousand intelligence documents by whistleblower **Edward Snowden** in 2013. These documents outline a large and comprehensive system with major technology companies being involved in actively monitoring and storing data, and a large reaction from the press followed. Protests against the NSA's surveillance programme (the programme encompassed a variety of codenames with a variety of different purposes, but some of the most important include **XKeyscore**, **PRISM**, and **Tempora**) cited violations of human rights to privacy and other legal crimes.

However, advocates of the global surveillance programme say that it is a necessary compromise in order to ensure national security. By monitoring the global communications network, intelligence agencies are better equipped to stop crime and acts of terrorism before they happen, and potential troublemakers can be monitored to prevent future crime.

There exists a trade-off between the amount of privacy we are willing to give up for security and vice versa. If you haven't done anything wrong, why should you care if the NSA monitors? What if someone oversteps in the NSA and accesses information without oversight? What kind of regulatory and overseeing bodies should intelligence agencies be subjected to? These are the kind of questions international players face today when dealing with the issue of global intelligence: *what compromises should be made to ensure national security?*

It's important for countries to consider these questions and devise appropriate legal and executive decisions to handle the issue.