Global Classrooms
International Model United Nations
High School Conference

The Legal Committee (GA6)

The Question of Digital and Cyber Surveillance on Civilians

2016 "LEAD BY EXAMPLE"
MAY 12-14

Description of the Committee

The sixth committee of the General Assembly is the main medium for international law. GA6 is the legal division of the United Nations General Assembly. All negotiations concerned with general law are held in GA6. All member states are allowed representation in GA6 since it is one of the main committees of the General Assembly. GA6 meets annually from late September to late November. In the meeting, several issues are discussed such as the reports of the International Law Commission, the UN Commission on International Trade Law, and actions that should be taken to eliminate international terrorism. Recommendations done by the sixth committee are then sent to the General Assembly Plenary to make the final decision.

History of Topic

Cyber surveillance is defined as the online monitoring of all internet activity done by civilians, and this includes any type of data uploaded, downloaded, or shared online. On the other hand, digital surveillance comprises close supervision through telephones, cameras, biometrics, aircrafts, satellite imagery and GPS. All these types of surveillance, interception and data collection can be performed by governments, enterprises, criminal groups, or even individuals.

Surveillance by governments is often done in order to prevent certain risks, monitor criminal activity, maintain social control, and foresee national threats. Due to the ongoing technological development and to the level of advancement that has been reached, it is now possible to monitor activity in live time, anywhere in the world.

However, this surveillance is often done secretly, and if not performed with approval from a court or an independent agency, it may be illegal. Concerns have been raised over this social control that violates the civilians' privacy. In fact, as cyber surveillance becomes more widespread and easier to do without being detected, it is a growing fear that governments are using it to suppress individual freedom.

Recently, many electronic mass-surveillance activities performed by different countries worldwide, notably the US and the UK, have been exposed. Governments have threatened to ban the services of telecommunication and wireless equipment companies unless given direct access to all their cables for surveillance purposes, and required companies to disclose information on customers and employees. There are reports that authorities in some States routinely record all phone calls and retain them for analysis. Furthermore, authorities in some countries require all personal computers sold in the country to be equipped with filtering software that may have other surveillance capabilities. Mass surveillance technologies are now entering the global market, raising the risk that digital surveillance will escape governmental controls.

Detailed Description

The right to privacy

Article 12 of the Universal Declaration of Human Rights provides that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." The same statement was also issued in article 17 of the International Covenant on Civil and Political Rights, ratified by 167 States.

The beginning of cyber surveillance

ECHELON, originally a code-name, was created by the USA, Great Britain, Canada, New Zealand and Australia, in 1947, to share the product of eavesdropping (i.e. secretly listening) on the world's nations. While for the first few decades of its existence, Echelon was primarily used for eavesdropping on military and diplomatic communications, especially during the Cold War, technological advances meant that Echelon can also monitor industrial targets and private individuals. Nowadays, it is estimated that monitored transmissions contain about 3 billion communications daily: this number includes phones calls, emails, faxes,

satellite transmissions, and internet downloads from citizens and companies worldwide. However, it seems that the main targets of ECHELON are not terrorists or politicians, but citizens themselves.

Recent outbreaks

Global concerns have been amplified following revelations in 2013 and 2014 that suggested that, together, the National Security Agency in the United States of America and General Communications Headquarters in the United Kingdom of Great Britain and Northern Ireland have developed technologies allowing access to much global internet traffic, calling records in the United States, individuals' electronic address books and huge volumes of other digital communications content. These technologies have reportedly been deployed through a transnational network comprising strategic intelligence relationships between Governments, regulatory control of private companies and commercial contracts.

International surveillance by the NSA and the case of Edward Snowden

The National Security Agency (NSA) provides information and strategies to American government and military leaders, and has been doing so for over half a century. By nature, the NSA requires a high degree of confidentiality.

In June of 2013, Edward Snowden, a government contractor, gave an interview to reporters from The Guardian, explaining that the National Security Agency has been secretly monitoring and collecting phone data from the American people. The NSA have been collecting massive quantities of information, including emails, phone numbers, instant messages, and contact information, which is being stored in government databases. Using this metadata, they create maps and social networks of identities, in order to find potential threats to national security or crisis. Further investigations uncovered evidence that devices belonging to heads of government, such as those of Germany and France, are also being monitored.

Snowden also revealed that the NSA has also been hacking into computers and collecting information from computers in Hong Kong and China since 2009. This means that the American government was monitoring American online data for threats, but also the private information of citizens from other countries: something that can be seen as a breach of national sovereignty.

Previous Actions

European Union

On the 13th December 2012, the European Union passed a resolution that banned exports from the European Union on technologies that could be used to conduct mass surveillance, track a person's movements or block information online. In the resolution, parliamentarians said that the European Union should focus on protecting and promoting digital rights in all of its external actions.

UN actions

Following on the concerns of Member States and other stakeholders at the negative impact of these surveillance practices on human rights, in December 2013, the General Assembly adopted resolution 68/167, without a vote, on the right to privacy in the digital age. In the resolution, which was co-sponsored by 57 Member States, the Assembly affirmed that the rights held by people offline must also be protected online, and called upon all States to respect and protect the right to privacy in digital communication. It further called upon all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data, emphasizing the need for States to ensure the full and effective implementation of their obligations under international human rights law.

Also in resolution 68/167, the General Assembly requested the United Nations High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session, with views and recommendations, to be considered by Member States. The present report is submitted pursuant to that request. As mandated by resolution 68/167, the Office of the High Commissioner for Human Rights (OHCHR) will also submit the report to the Assembly at its sixty-ninth session.

On that note, the United Nations High Commissioner for Human Rights Navi Pillay released a far-reaching report on July 16, 2014 warning that, globally, "mass surveillance [is] emerging as a dangerous habit rather than an exceptional measure" and reaffirming that state

surveillance may only be conducted if it is necessary and proportionate to a legitimate goal. The report criticizes many common practices and justifications offered by the US, UK, and other governments in support of mass surveillance.

Furthermore, the OHCHR took many actions in order to protect the right to privacy in the digital age.

Relevant UN treaties:

- Written statement submitted by Reporters without Borders International, a nongovernmental organization, 13 June 2012 (A/HRC/20/NGO/3)
- The promotion, protection and enjoyment of human rights on the Internet, 16 July 2012, (A/HRC/RES/20/8)
- Protection of human rights and fundamental freedoms while countering terrorism, 11 April 2014, (A/HRC/RES/25/7)

Other actions

- The Electronic Frontier Foundation (EFF) is an NGO focused on defending civil liberties in the digital world. They work to ensure that rights and freedoms are advanced as technology continues to grow.
- Big Brother Incorporated (BBI): in countries where detention without trial, torture and extrajudicial killings are legal, exporting surveillance technology to them can help further the agendas of oppressive regimes and the citizens of that country at risk. With the advances made in surveillance technology, governments can use them to facilitate large scale social control. BBI investigates companies that produce such technologies and the networks that allow for them to be sold to oppressive regimes in order to abuse human rights. BBI encourages governments to regulate the surveillance industry and to use export control systems to make sure that surveillance technology products are not traded.
- Global Online Freedom Act 2012 (GOFA) :
  While there have been previous versions of the GOFA act, this one is an important step in protecting human rights and freedom of expression online. It requires government assessments of the "freedom of expression with respect to electronic information in each foreign country," requires companies to disclose their human rights practices to independent third parties who will evaluate them, and to limit the export of technologies that have the primary purpose of allowing governments to commence with mass surveillance.

Recommendations/ Questions

When is electronic surveillance necessary?

Several contributions highlighted that, when conducted in compliance with the law, including international human rights law, surveillance of electronic communications data can be a necessary and effective measure for legitimate law enforcement, intelligence purposes, and counter-terrorism measures.

When does electronic surveillance become problematic?

Revelations about digital mass surveillance have, however, raised questions around the extent to which such measures are consistent with international legal standards and whether stronger surveillance safeguards are needed to protect against violations of human rights. Specifically, surveillance measures must not arbitrarily or unlawfully interfere with an individual's privacy, family, home or correspondence. Governments must take specific measures to ensure protection of the law against such interference.

Ban on selling surveillance technologies to authoritarian regimes

Countries should take steps to ban the exportation of surveillance products and tools to countries with known histories of extreme cyber surveillance. However, to completely shut down the export of surveillance products might hurt the technology industry, and as a result, hurt the economy of the country.

In order to avoid such a consequence, a list should be released, detailing countries that are known to perform online surveillance on citizens. It is ideal that such a list should be made by a neutral party, such as the United Nations, or an NGO. Once such a list has been made, countries can then create bans on exporting surveillance tools and services to countries that are on the list, making it punishable by law to provide the tools for online surveillance. Alongside creating a list of countries that perform internet surveillance, reasons should be given as to why such countries are included on the list, as well as reasons for why countries are not on the list.

Further Questions

- Does the government of your country conduct cyber and digital surveillance on civilians? If yes, is it lawful and justifiable? To what extent is it transparent?

- Is your country in need of legal cyber surveillance technologies to

better regulate crimes and ensure social security?

- What are the motives and strategies of digitally mediated surveillance (DMS) actors?

- What do people know about the DMS practices and risks they are exposed to in everyday life? What are people's attitudes to these practices and risks?

- Is a re-evaluation of traditional information privacy principles required in light of new and emergent online practices, such as social networking and others?

- What is the role of activist movements in challenging cyber-surveillance?

- How can we draw the line between the necessary surveillance, in order to promote national and international security, and unjustifiable surveillance performed solely for the purpose of ensuring the special interests of some political, governmental or individual parties?

Citations

https://www.eff.org/issues

http://www.hrw.org/news/2014/07/17/united-nations-rein-mass-surveillance

http://cyfy.org/event/rethinking-media-freedom-in-a-digital-age/

http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

https://www.eff.org/press/releases/thirteen-principles-against-unchecked-surveillance-launched-united-nations

http://www.un.org/apps/news/story.asp?NewsID=45075#.VOySJfmUdjI