Research Report

Leiden Model United Nations 2017
~ fresh ideas, new solutions ~

Forum: *General Assembly Fourth Committee*
Issue: *International internet surveillance*

Position: *Chair*

Introduction

We live in a digital age, the age of information. Access to this information has put governments in a position of yet unprecedented power, and as always, with great power comes great responsibility; a responsibility to handle that information accordingly. But what if governments do not handle accordingly, and exploit their access to people's information for unclear motives? We are told that if we have nothing to hide we should have nothing to fear, but according to the United Nations' High Commissioner on Human Rights these shadowy government bodies threaten our right to privacy, association and freedom of speech declared by the Universal Declaration of Human Rights. Can the means justify the goal if international internet surveillance is capable of removing our fear of terror, or is our privacy too valuable to waver?

Definition of Key Terms

Targeted surveillance
Monitoring targeted on specific persons of interest.

Mass/Bulk surveillance
The subjection of a population or significant component of a group to indiscriminate monitoring.

Snowden documents
The documents published by whistleblower Edward Snowden in June 2013. The documents expose the mass surveillance carried out by the United States and the United Kingdom, which infringe multiple rights dictated by the Declaration of Human rights.

General Overview

With Edward Snowden's leaks the world got its first look at the scope of surveillance carried out by the United States' National Surveillance Agency (NSA) and its British counterpart the Government Communications Headquarter (GCHQ). What was revealed was that despite being part of the Freedom Online Coalition, a coalition of countries promoting online privacy, both these nations had set up Surveillance agencies that were capable of mass surveillance of data both domestic and international on an immense scale. This type of mass surveillance of data goes against the UN's International Covenant on Civil and Political Rights, of which article 17 states that "no one shall be subject to arbitrary or unlawful interference with his or her privacy, family, home and correspondence, nor to unlawful attacks on his or her honour and reputation". In other words, governments are allowed to target specific individuals with their surveillance if they have sufficient reason to believe that this individual is going to break their laws, however they may not use mass surveillance to check on all internet traffic in hopes of finding an individual planning or preforming illegal activities.

So far the NSAs and GCHQs mass surveillance has had little effect. Up until now 0 major terror attacks have been prevented by their surveillance systems. After the 9/11 terror attacks the United States' Federal Bureau of Investigation used NSA mass surveillance records to hold 5000 American Citizens in preventive detention, however none of them proved to be terrorists. Furthermore, the Snowden Documents also revealed that NSA policy has weakened encryption standards and withheld information about security holes in order to utilise them for its own benefits. On the other hand surveillance agencies have always been limited by national and international laws as well as funding. If agencies were able to operate at their full potential and on a more international level, they might be able to pre-emptively stop terrorist attacks and provide governments with useful information about national security.

According to a survey carried out by Privacy International in 2007 18 countries indulged in mass surveillance, however it is often unclear to what extent.

The media have also taken a stand on this issue. Journalists often have to protect their sources and value their internet privacy very much. Furthermore non-government-controlled media feel that surveillance limits their ability to report in an unbiased way. Besides the media also stand big corporations that are responsible for their users' privacy. The loss of trust in governments' surveillance programmes led them to encrypt their data. In September 2014 Apple and Google announced that their users' data would not be accessible to neither company nor government. Other companies like Microsoft, Yahoo and Facebook have also taken steps to protect their data from governments. It is therefore important that they are taken into consideration when it comes to solving this issue. The Snowden Documents did however reveal that the NSA can demand user data from large tech companies in the US, which are by law compelled to comply.

So should we collectively take measures to halt the ascent of surveillance agencies, implement safeguards and set new standards for privacy? Or should measures be taken to promote the coverage of surveillance agencies trough amending treaties and looser regulations? The real question we need to ask ourselves is whether what we profit from International Internet Surveillance is capable of covering its costs.

Major Parties Involved

USA
Since the publishing of the Snowden documents the USA has done very little to reign in the scale of surveillance, despite massive international criticism. The USA argues that as the leader of the Free World it needs surveillance to ensure national and international security and often utilises it in conflict areas where it is involved. To carry out its surveillance it uses the government controlled NSA.

UK
The UK has always remained very secretive about its surveillance body, the GCHQ. Even after the publishing Snowden documents they refused to answer even the most basic questions about its intelligence gathering practices. In 2014, one year after the leaks, the UK government even passed a law that extended the surveillance powers.

Human Rights Watch
Human Rights Watch has worked hard to expose the dangers of surveillance by governments and to warn the international community of those dangers through reports.

Possible Solutions

Since most governments profit from their surveillance agencies it will be hard to convince governments to make changes to their policies. However governments too answer to UN laws and declarations. Therefore certain changes can be made to improve transparency of surveillance agencies, for instance the setting up of a watchdog body or investigation committee.

Another solution could be to tackle the problem at its root, and prevent surveillance agencies from getting their information in the first place. This could by done through the setting of better standards for encryption of user data by tech companies and a general raising of awareness.

Yet another solution could be the drafting of an international treaty that specifies the limits to surveillance and sets clear guidelines for governments on the instalment of new safeguards secure civil privacy rights.

Useful documents

Human Rights Watch report on Government Surveillance:
https://www.hrw.org/world-report/2015/country-chapters/global-0#531a45
Extent of The Right to Privacy in the Digital Age:
http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
Analysis of International Privacy:
https://www.privacyinternational.org/blog
A short introduction to surveillance:
https://www.youtube.com/watch?v=V9_PjdU3Mpo

Appendix/Appendices

https://www.freedomonlinecoalition.com/about/members/
https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/1-The-Hague-FOC-Founding-Declaration-with-Signatories-as-of-2013.pdf
https://www.theguardian.com/world/2014/oct/15/internet-surveillance-report-edward-snowden-leaks
http://www.reuters.com/article/us-privacy-un-idUSKBN16F1M3
https://en.wikipedia.org/wiki/Mass_surveillance
http://www.un.org/en/universal-declaration-human-rights/
https://www.privacyinternational.org/node/12
http://mashable.com/2014/06/05/edward-snowden-revelations/#sJhifGk2UPqZ
http://www.popsci.com/article/technology/edward-snowden-how-end-mass-surveillance
https://theintercept.com/2014/10/15/un-investigator-report-condemns-mass-surveillance/