

Forum: Human Rights Council

Issue: Privacy in the digital age

Student Officer: Therese Steffensen

Position: Co-chair

## Introduction

The Human Rights Council is an inter-governmental body within the United Nations system made up of 47 States responsible for the promotion and protection of all human rights around the globe. It has the ability to discuss all thematic human rights issues and situations that require its attention throughout the year. It meets at the UN Office at Geneva. It works to make sure that all people know about their rights; all people can use their rights. Rights are things that should happen for everyone, everyone has the rights to live; be treated fairly; go to school; free voting procedures in elections and/or other political decisions.

There are different things that The Human Rights Council does, including making sure that people understand their rights, have the same rights, can use their rights, check what is done in the government to protect the rights of people in a country, and help those people whose rights were taken away. For specifically this session, the discussion of privacy in the digital age will be addressed, addressing the rights to privacy and how it can be strengthened.

## Definition of key terms

The Right to Privacy - As defined by Universal Declaration of Human Rights, “No one shall be subjected to arbitrary or unlawful interference with his/her privacy, family, or correspondence, or to unlawful attacks on his/her honor and reputation.”

Internet Censorship - “Control or suppression of what can be accessed, published, or viewed on the Internet enacted by regulators, or on their own initiative.”

Edward Snowden - Former National Security Agency subcontractor. Leaked top secret information about NSA surveillance activities.

Golden Shield Project - A system that prevents access to websites deemed undesirable by the government of the People's Republic of China

Christopher Wylie - Former director of research at Cambridge Analytica. Canadian whistleblower in the Facebook–Cambridge Analytica data scandal

Whistleblower - A person who informs on a person or organization regarded as engaging in an unlawful or immoral activity.

Net Neutrality - The principle that Internet service providers should enable access to all content and applications regardless of the source, and without favouring or blocking particular products or websites.

Myspace - a social networking website offering an interactive, user-submitted network of friends, personal profiles, blogs, groups, photos, music, and videos.

## General overview

Privacy is the “right to be free from unwarranted intrusion and to keep certain matters from public view”. The rapid pace of technological development enables individuals all over the world to use new information and communications technologies (ICTs) to improve their lives. At the same time, technology is enhancing the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy. As with previous UN resolutions on this topic, the resolution adopted on 21 November 2016 recognises the importance of respecting international commitments in relation to the right to privacy.

Recognising that more and more personal data is being collected, processed, and shared, the resolution expresses concern about the sale or multiple re-sales of personal data, which often happens without the individual’s free, explicit and informed consent. It calls for the strengthening of prevention of and protection against such violations, and calls on states to develop preventative measures, sanctions, and remedies.

In the expanding surveillance industry, it is common to spy on citizens. “American, British and Allied intelligence agencies are soon to embark on a massive, billion-dollar expansion of their global electronic surveillance system.” This will allow the agencies to monitor current communications between citizens, and possibly intercept them. A strong barrier of high technology protects such agencies, and there are currently no measures taken against them. The scandals about governments taking unauthorized information from their citizens lead to general awareness about rights to privacy. People no longer trust their nation’s government, and therefore the public continues to want more transparency on this issue.

Internet censorship has been apparent in the recent years, and is usually carried out through national governments. Most countries have moderate Internet censorships, however some are more severe than others. Some governments decide to block sites, limiting access to news broadcasts, for example, or place restrictions on internet users because of social, religious and commonly, political reasons. Internet censorships may also occur because of anticipation of certain events such as protests or riots. An example of this is Arab Spring, which started in Tunisia in 2010 before spreading to other Arab countries. It happened at the time that many protests broke out. The government shut down some social media sites, as they feared that their citizens were communicating and spreading ideas between countries, online.

A prime example of extreme Internet censorship is in China. They have the license to shut down sites through the Public Pledge on Self-Discipline for the Chinese Internet. Not only does the government block sites, such as Facebook and Twitter in 2009, but they also monitor individual’s uses of the Internet. Many sites hire internal staff themselves to complete this monitoring for the government. Their job is to scan chat forums, in which the citizens are unaware of, to search for inappropriate comments on the country's political status. They are known to place fines and imprisonment for ‘unacceptable’ uses of the internet.

Twitter is currently blocked in North Korea, China and Iran. It was blocked in Turkey for a long time, due to the spreading of videos, which insulted the country's founder, Mustafa Kemal Atatürk. The ban from the Turkish government was released 2 weeks after it was implemented, but it continued to block 2 users who pointed out political and economic problems with the country.

## Timeline of key events

December 10th, 1948 - Universal declaration of Human Rights was adopted

October 24th, 1995 - EU released a directive on the protection of individuals with regards to the processing of personal data and on the free movement of such data

June, 1997 - The Electronic Privacy Information Center reports 17 out of the 100 most popular internet sites have privacy policies

March 16th, 2002 - The Internet Society of China launched the Public Pledge on Self Discipline for the Chinese Internet Industry

November 2003 - The Golden Shield Project was launched

April 2007 - A Chinese version of Myspace was launched in which all political comments were banned

Lte 2009 - The Chinese government blocked social media sites such as Facebook and Twitter

December 17th, 2010 - First outbreak of protests in Tunisia, starting the 'Arab Spring'

January 25th, 2012 - Reform of the EU's data protection rules to strengthen online privacy rights and boost Europe's digital economy was released

June, 2013 - Edward Snowden leaked classified information from the US NSA to the media

March 20th, 2014 - Twitter was blocked in Turkey

July, 2014 - Russian President Vladimir Putin signed the new personal-data measures in to law

September, 2014 - OHCHR presented their report on the Right to privacy in the Digital Age to the Human Rights Council

March 17th, 2018 - Christopher Wylie, former employee at Cambridge Analytical turned whistleblower, presents information on how Cambridge Analytical and Facebook collect personal data information on 87 million Facebook users

May 2018 - EU implemented new privacy law called G.D.P.R, providing one set of data protection rules for all companies operating in Europe

## Majorly involved parties

### United States

On the 28th of March, 2017, House of Representatives voted to repeal an Obama-era law that demanded ISPs have permission to share personal information - including location data. The Net Neutrality rules expired on June 11th, 2017, where a new set of rules was implemented. The prior rules were intended to ensure a free and open internet, give consumers equal access to web content and bar broadband service providers from favoring their own material or others. The new rules require internet providers to tell consumers whether they will block or slow content or offer paid "fast lanes." The current President Donald Trump signed the repeal on New Neutrality laws.

## **United Kingdom (UK)**

In a statement of intent the Government has committed to updating and strengthening data protection laws through a new Data Protection Bill. It will provide everyone with the confidence that their data will be managed securely and safely. Research shows that more than 80 per cent of people feel that they do not have complete control over their data online. Matt Hancock, Minister of State for Digital said “Our measures are designed to support businesses in their use of data, and give consumers the confidence that their data is protected and those who misuse it will be held to account.”

## **European Union (EU)**

In May 2018, the European Union General Data Protection Regulation was accepted. It was an replacement for the 1995 Data Protection Directive. This offered users to have control over what companies gather about the user, and even see what type of data is collected. The basic idea behind the law is to orient companies toward “privacy by default” and put people in charge of their personal data. The European Court of Justice ruled in 2014 that European citizens have a “right to be forgotten” and can have material stricken from search engines if it is determined to be “inaccurate, inadequate, irrelevant, or excessive for the purpose of the data processing,” a ruling enshrined in GDPR as well.

## **People’s republic of China**

China is the major party in Internet censorship worldwide. They are known to be strict and controlled in what they are allowing their citizens to see. Certain websites that the government deems potentially dangerous—like Wikipedia, Facebook, Twitter, YouTube, and some Google services—are fully blocked or temporarily “blacked out” during periods of controversy, such as the June 4 anniversary of the Tiananmen Square massacre or Hong Kong’s Umbrella Movement protests in the fall of 2014. The Chinese government has a system called “social credit”, ratings on citizens based on governmental data, determining the “trustworthiness” of a person. Social credit is preventing people from buying airline and train tickets, stopping social gatherings from happening, and blocking people from going on certain dating websites. Meanwhile, those viewed as trustworthy are rewarded with discounted energy bills and similar perks.

## Previous attempts to resolve conflict

The Office of the High Commissioner for Human Rights (OHCHR) looks over major programs in protecting human rights internationally. Following the concern of the UN General Assembly on this issue, they created a report on digital privacy, which was presented in September 2014 and further discussed in the resolution of the General Assembly in December 2014. Furthermore, there have been multiple panels in the Human Rights Committee on this issue.

- Universal Declaration of Human Rights, 10 December 1948
- Developments in the field of information and telecommunications in the context of international security, 9 January 2014
- The Right to Privacy in the Digital Age, 18 December 2014
- The EU implementing G.D.P.R, May 2018

## Possible solutions

Placing effective laws against issues such as the Facebook incident, will not only raise awareness of the issue but also hopefully decrease the number of such events happening again. It is also important to keep such legislative bodies up to date with updates that cover recent and emerging technologies.

Placing harder and more effective penalties upon hackers and/or whistleblowers, or towards a person with unauthorized access to private information. Penalties currently are between fines and/or prison time, depending on the level of misuse of data. Edward Snowden receiving 30 years in prison from the US government; many still believed he deserved lifetime or even death sentence.

More recognition towards whistleblowers. Whistleblowers bring attention to large corporations that abuse their power, and therefore some believe they should be congratulated. This could include, for example, giving them protection or economic help

## Bibliography

RM Long, William, et al. "United Kingdom - The Privacy, Data Protection and Cybersecurity Law Review - Edition 4." *The Law Reviews*, 2017, [thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151345/united-kingdom](http://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151345/united-kingdom).

"Government to Strengthen UK Data Protection Law." *GOV.UK*, GOV.UK, 6 Aug. 2017, [www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law](http://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law).

Cooper, Dan. "The UK Adopts Data Protection Act 2018." *Inside Privacy*, 25 May 2018, [www.insideprivacy.com/international/united-kingdom/the-uk-adopts-data-protection-act-2018/](http://www.insideprivacy.com/international/united-kingdom/the-uk-adopts-data-protection-act-2018/)

Clare. "Online Privacy Law: United Kingdom." *Apple Computers: This Month in Business History (Business Reference Services, Library of Congress)*, Victor, 1 Dec. 2017,

[www.loc.gov/law/help/online-privacy-law/2017/uk.php](http://www.loc.gov/law/help/online-privacy-law/2017/uk.php).

Brodkin, Jon. "Trump Hits Campaign Trail to Endorse Key Foe of Net Neutrality Rules." *Ars Technica*, Ars Technica, 30 May 2018, [arstechnica.com/tech-policy/2018/05/trump-hits-campaign-trail-to-endorse-key-foe-of-net-neutrality-rules/](http://arstechnica.com/tech-policy/2018/05/trump-hits-campaign-trail-to-endorse-key-foe-of-net-neutrality-rules/).

Romm, Tony. "The Trump Administration Just Eliminated the U.S. Government's Net Neutrality Rules." *Recode*, Recode, 14 Dec. 2017, [www.recode.net/2017/12/14/16771910/trump-fcc-ajit-pai-net-neutrality-repeal](http://www.recode.net/2017/12/14/16771910/trump-fcc-ajit-pai-net-neutrality-repeal).

Watts, Mark. "Practical Law." *Practical Law UK Signon*, 2017, [uk.practicallaw.thomsonreuters.com/3-525-6372?transitionType=Default](http://uk.practicallaw.thomsonreuters.com/3-525-6372?transitionType=Default).

Madrigal, Alexis C. "What We Know About Facebook's Latest Data Scandal." *The Atlantic*, Atlantic Media Company, 5 June 2018, [www.theatlantic.com/technology/archive/2018/06/what-we-know-about-facebooks-latest-data-scandal/561992/](http://www.theatlantic.com/technology/archive/2018/06/what-we-know-about-facebooks-latest-data-scandal/561992/).

"HOW TO TALK ABOUT THE RIGHT TO PRIVACY AT THE UN." *Official UN Guide*, 2017, [privacyinternational.org/sites/default/files/2017-12/UN\\_Guide\\_Final.pdf](http://privacyinternational.org/sites/default/files/2017-12/UN_Guide_Final.pdf).

"United Nations Official Document." *United Nations*, United Nations, 2016, [www.un.org/ga/search/view\\_doc.asp?symbol=A%2FC.3%2F71%2FL.39%2FRev.1](http://www.un.org/ga/search/view_doc.asp?symbol=A%2FC.3%2F71%2FL.39%2FRev.1).

Bremmer, Ian. "GDPR Day: How Countries Are Handling Digital Privacy Rights." *Time*, Time, 25 May 2018, [time.com/5291529/gdpr-digital-privacy/](http://time.com/5291529/gdpr-digital-privacy/).

Xu, Beina, and Eleanor Albert. "Media Censorship in China." *Council on Foreign Relations*, Council on Foreign Relations, 2017, [www.cfr.org/backgrounder/media-censorship-china](http://www.cfr.org/backgrounder/media-censorship-china).

Tannam, Ellen. "Privacy Worries Increasing among Internet Users in China." *Silicon Republic*, 8 Jan. 2018, [www.siliconrepublic.com/enterprise/china-online-privacy-tencent-alibaba](http://www.siliconrepublic.com/enterprise/china-online-privacy-tencent-alibaba).

Diamond, Anna Mitchell Larry. "China's Surveillance State Should Scare Everyone." *The Atlantic*, Atlantic Media Company, 5 Feb. 2018, [www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/](http://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/).

“2018 Reform of EU Data Protection Rules.” *Social Protection Statistics - Unemployment Benefits - Statistics Explained*, 20 June 2018,  
[ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-da  
ta-protection-rules\\_en](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en).

Powles, Julia. “The G.D.P.R., Europe's New Privacy Law, and the Future of the Global Data Economy.” *The New Yorker*, The New Yorker, 25 May 2018,  
[www.newyorker.com/tech/elements/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-  
data-economy](https://www.newyorker.com/tech/elements/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy).