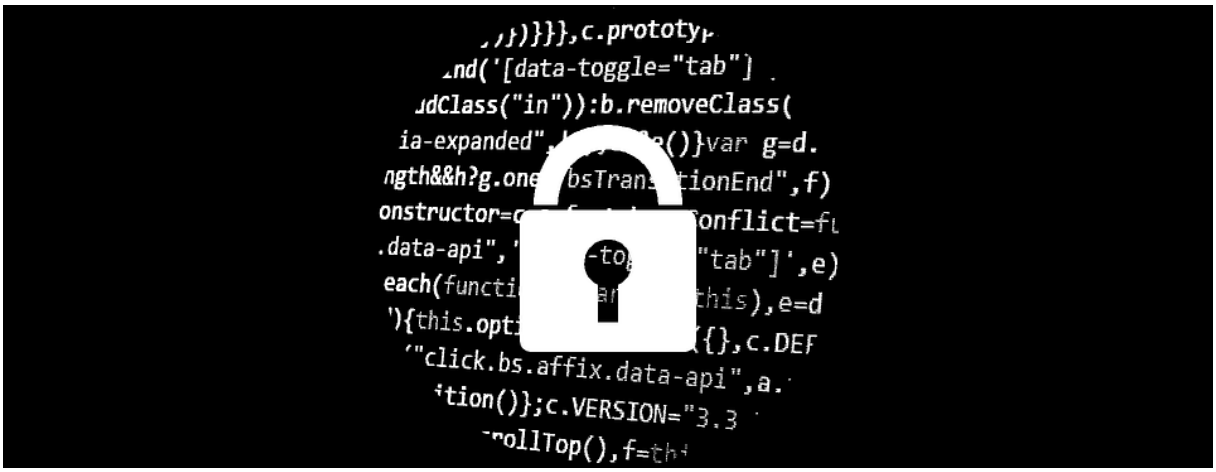
The International European Model United Nations 2018



Human Rights Council

Topic B: Privacy in the Digital Age

Ivy Omondi and Romee Lutterop

Welcome letter by the chairs

Dear delegates,

On behalf of The European International Model United Nations, we would like to welcome you to the Human Rights Council. We look forward to being your chairs and making your Model United Nations experience worth remembering!

Participating as a delegate in TEIMUN may be a challenging, but definitely rewarding experience for you. We are certain that this Council will present opportunities for each and every delegate to learn, excel, and broaden their horizons. In and out of session, you will be pushed to consider innovative solutions to modern issues facing the international community. Outside of the committee room, you will have the opportunity to interact while making friends from around the world.

With the challenges concerning human rights growing increasingly pressing, the HRC's responsibilities have increased dramatically over the past years. More than any other Council, HRC faces the immense task of uniting nations to solve problems truly global in scope. At the same time, regional issues, smaller in scope yet just as pressing, demand solving, too. As such, as your chairs we expect you, delegates of HRC, to give your best effort while respecting the rules of procedure and your fellow delegates. We hope that TEIMUN will be an amazing experience for all of you, and that besides the challenging debates and having a blast, you will make connections and friends that will last for a lifetime. We are very much looking forward to meeting you in The Hague come July 2018!

Your chairs,

Ivy Omondi

E-mail: ivy.shiechelo@strathmore.edu

Romee Lutterop

E-mail: romeelutterop@gmail.com

Facebook group: https://www.facebook.com/Teimun2018UNHRC/
General council mail: hrc@teimun.org

Index

"You have zero privacy anyway. Get over it."[1]

-Scott McNealy,

chief executive officer of Sun Microsystems

Introduction

As of January 2017, 50 percent of the global population has access to the Internet.[2] With recent advancements in technology and the greatest expansion of access to information and communication in history, international human rights law remains relevant and applicable. In particular, the provisions relating to the right to privacy have become more important than ever. Both states and private parties have the power to cripple privacy online, which raises questions on the rights and responsibilities of public authorities and private actors, especially since privacy and other human rights issues often overlap. Additionally, surveillance capabilities have outstripped the ability of laws to effectively regulate it. The grey area between the regulation of the Internet and the protection of the peoples' privacy is vague, which has resulted in instances of human rights violations. Oftentimes these violations occur between the right to security and the right to privacy.[3] The UN has not established where the limit to privacy in the digital age is, and at what point (if any) a violation of this right would be preferable to a violation of the right to security. There is a grey area between these human rights where governments and organizations try to ensure security by monitoring online presences of potential threats or civilians in general, which can be seen as a necessary invasion of privacy to ensure security, or seen as a violation of the human right to privacy. Furthermore, it is not clear if there is a difference between privacy online and offline or whether the online sphere is simply a continuation of the offline violations of the right to privacy. As Scott McNealy said specifically about violations of digital privacy: "You have zero privacy anyway. Get over it."[4] The role of the UNHRC is to figure out to what extent this might be true and how the human right of privacy can be protected in the digital age.

Privacy (in the digital age)

There is not a set definition of privacy as provided by the United Nations, but the definition that is generally used is "the presumption that individuals should have an area of autonomous

[1] Sprenger, P. "Sun on Privacy: 'get over it'. Wired News. 1999. https://www.wired.com/1999/01/sun-on-privacy-get-over-it/
[2] Statista, "Online Privacy – Statistics and Facts." 2017. Paragraph 1. https://www.statista.com/topics/2476/online-privacy/
[3] The United Nations. Universal Declaration of Human Rights. 1948. Article 19.
[4] Sprenger, P. "Sun on Privacy: 'get over it'. Wired News. 1999. https://www.wired.com/1999/01/sun-on-privacy-get-over-it/

development, interaction and liberty, a 'private sphere' with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals."[5] The United Nations has also not set out the different types and forms of privacy as well as violations of these. Some facets of privacy may include:

i. Information Privacy (for example: identity information, credit information and medical records);
ii. Bodily privacy (for example: drug testing and cavity searches;)
iii. Privacy of communications (for example: mail, telephones, email and other forms of communication); and
iv. Territorial privacy (for example: intrusion into home, workplace and public space).[6]

In relation to digital privacy, information privacy and privacy of communications are most commonly violated online. Since the advancement of technology, people use their identity information and credit information online, while doctors often have online medical files. Conversations can be held online, saved online or can be accessed by third parties online, which would violate the privacy of communications. It is also possible, however less common, to have an intrusion into territorial privacy, if one's workplace or public space is online. Such an intrusion of digital privacy can be ordered by the government on its own people, terrorist suspects, foreign leaders and foreign citizens in the form of surveillance. Additionally, private organizations and individuals can also gain information online that citizens did not agree to, as will be explained later.

Background of the issue

In 2018 the United Nations celebrates the 70th anniversary of the adoption of the Universal Declaration of Human Rights, which set out a universal core of human rights and fundamental freedoms for the first time, including those on privacy.[7] Digital communications technologies such as the Internet have become part of everyday life, which has enhanced the capability of governments, organizations and individuals to conduct surveillance, data collection and regulate digital expressions, thereby violating human rights like the right to privacy.

Surveillance was common during the Cold War and the monitoring of civilians was widespread and intrusive. Technological developments in information technology (IT) in the 1960s and 1970s especially have increased the power of surveillance. This raised more possibilities of potential human rights violations than before, since information was now more

[5] Lord Lester and D. Pannick (eds.). Human Rights Law and Practice. London, Butterworth, 2004, para. 4.82.
[6] Privacy International, "PRIVACY AND HUMAN RIGHTS An International Survey of Privacy Laws and Practice", paragraph 23: Defining Privacy. http://gilc.org/privacy/survey/intro.html#fnlnk0009
[7] The United Nations. Universal Declaration of Human Rights. 1948. Article 12.

easily available than ever before to surveillance agencies. This information can result in even further human rights abuses by using it for offensive, military and illegal purposes. This has "prompted demands for specific rules governing the collection and handling of personal information" to avoid these abuses.[8]

Before the invention of the Internet, invading privacy via a computer required physical access to the computer. The Internet connected computers and streamlined the flow of knowledge online, but also created a new way to invade privacy or the security of computer systems by means of accessing or taking information that should not be public since they are vulnerable to electronic surveillance and interception. These violations can be performed through illegal means like viruses and hacks, but also through the tracking of users' behaviour by collecting data through 'cookies' without the users' permission or knowledge.[9] By the end of the 21st Century, both online identity theft and spyware were common.

These violations were generally assumed to be relatively small-scale and obvious to the public. However, this proved to be a minimization of the issue's importance, as illustrated by the 2013 "leak of operational details about the United Sates National Security Agency (NSA) and its international partners' global surveillance of foreign nationals and U.S. citizens."[10] The leaks by Mr. Edward Snowden revealed that American technical capabilities now included the ability to monitor computers that are not connected to the Internet and that the NSA has the ability to collect Americans' phone records and online history, and keep surveillance of foreign nations, all in the name of cybersecurity. Furthermore, it showed that the United States is not the only country that has agencies like the NSA in place, as surveillance systems used for "surveillance and social control" exist in many countries, including Uganda, Great Britain, Saudi Arabia, Iran, South Africa, the Soviet Union and more.[11][12] It is now public knowledge that internationally, there are many countries that have mass surveillance agencies or technology in place. The UN's special rapporteur on counter-terrorism, Ben Emmerson QC, stated that "mass surveillance of the Internet by intelligence agencies is corrosive of online privacy and threatens to undermine international law," which

[8] Privacy International, "PRIVACY AND HUMAN RIGHTS An International Survey of Privacy Laws and Practice", paragraph 36: The Evolution of Data Protection. http://gilc.org/privacy/survey/intro.html#fnlnk0009
[9] Aladeokin, Adeyemi, Pavol Zavarsky and Neelam Memon, "Analysis and compliance evaluation of cookies-setting websites with privacy protection laws," *2017 Twelfth International Conference on Digital Information Management (ICDIM)*, Fukuoka, 2017, pp. 121-126. https://ieeexplore.ieee.org/abstract/document/8244646/
[10] Statista. "Online Privacy – Statistics and Facts." 2017. Paragraph 3. https://www.statista.com/topics/2476/online-privacy/
[11] Greenwald, Glenn. "Revealed: how US and UK spy agencies defeat internet privacy and security." The Guardian. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[12] Privacy International. "The Global Surveillance Industry." 2016. Page 8, 9. https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

means the rapporteur believes these countries' mass surveillance agencies and technologies are detrimental to privacy and international law.[13]

While many countries across the world have programs of surveillance, they do not all cross the line to a violation of privacy rights for citizens. The Pew Research Center held a poll where citizens from countries all over the world responded to different types of mass surveillance, from monitoring your own citizens, foreign citizens, foreign leaders and terrorist suspects. They reported on the results on a global scale, but also included the results for individual country's citizen's opinions of mass surveillance in the United States.[14][15] This survey shows the international community largely disapproves of mass surveillance on different levels.

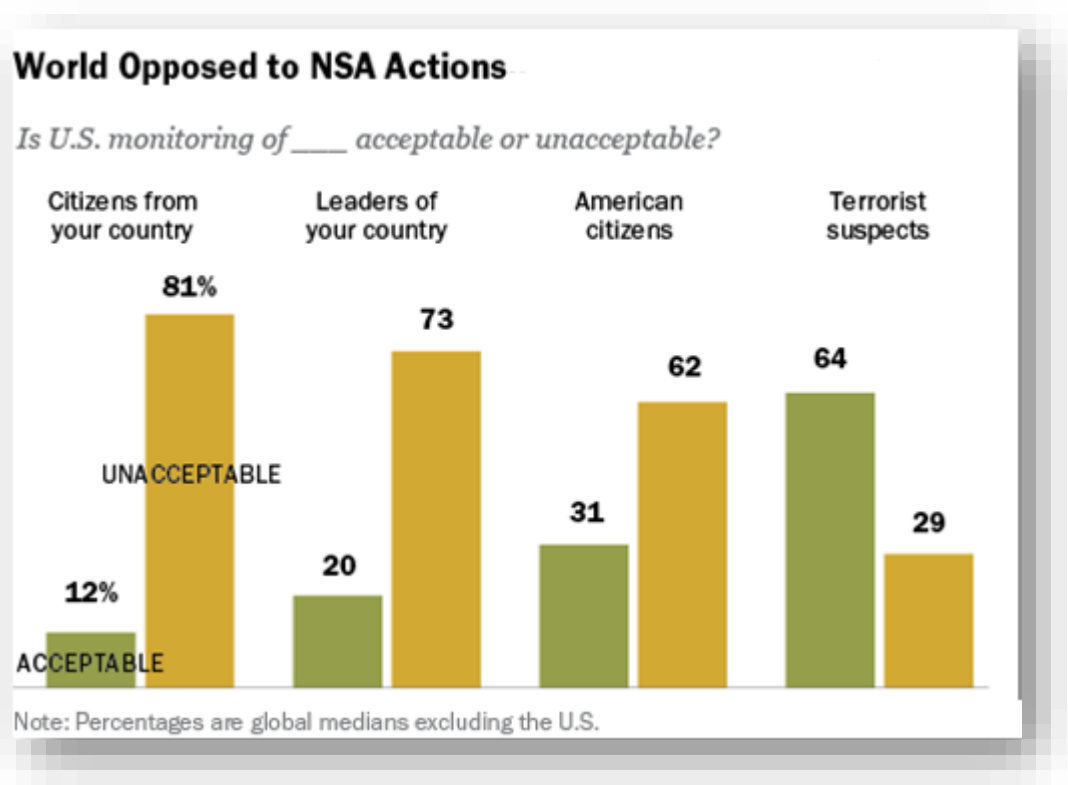


Figure 2: Pew Research Center. "Global Opposition to U.S. Surveillance and Drones, but Limited Harm to America's Image." 2014. Page 4. http://assets.pewresearch.org/wp-content/uploads/sites/2/2014/07/2014-07-14-Balance-of-Power.pdf.

[13] The United Nations. A/69/397. 2014. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement

[14] Pew Research Center. "Global Opinions of U.S. Surveillance." 2014. http://www.pewglobal.org/2014/07/14/nsa-opinion/

[15] Note: On http://www.pewglobal.org/2014/07/14/nsa-opinion/ you can view specific countries' people view of U.S. mass surveillance by clicking on the headings (Survey Country) Citizens, (Survey Country) Leaders, American Citizens and Suspected Terrorists in the graph itself.

Recently, Facebook has become the subject of outrage in the face of loss of digital privacy. This started when companies started to be able to "track purchases by Facebook users and notify their Facebook friends of what had been bought – many times without any user consent."[16] The publication of user information without warning nor consent has since been a staple of Facebook's privacy issue. In 2018, more issues with the right to privacy by Facebook were brought to light. In February, a Belgian court ordered Facebook "to stop collecting private information about Belgian users on third-party sites through the use of cookies," which means Facebook collected information on sites where people were unaware they could access information from.[17][18] Arguably the biggest issue Facebook has had with digital privacy was revealed in March of 2018, when it was revealed that "Facebook knew about [a] massive data theft and did nothing".[19] As exposed by the Guardian newspaper, millions of "Facebook profiles were harvested for Cambridge Analytica in a major data scandal".[20] This issue has exemplified once again how breaches of privacy online can go unnoticed and have great influence on the lives of individuals.

However, not only organizations perform these types of covert surveillance. For example, the Ethiopian authorities have "doubled down on its efforts to spy on its critics," which threatens "the privacy and the digital security of the people targeted".[21] The spyware offense started when a 10-month state of emergency was declared in 2016 with violent responses to "largely peaceful protests," and the Ethiopian authorities targeted foreign and native critics with infective spyware in order to spy on them.[22] As the writers of the report that uncovered the spyware explained: "in the absence of stronger norms and incentives to induce state restraint, as well as more robust regulation of spyware companies," they expect

[16] Newcomb, Alyssa. "A timeline of Facebook's privacy issues – and its responses." NBC News. 2018. Paragraph 8. Accessed on 27/3/2018. https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651
[17] Newcomb, Alyssa. "A timeline of Facebook's privacy issues – and its responses." NBC News. 2018. Par 23. Accessed on 27/3/2018. https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651
[18] Reuters Staff. "Facebook loses Belgian privacy case, faces fine of up to $125 million." Reuters. 2018. Accessed on 27/3/2018. https://www.reuters.com/article/us-facebook-belgium/facebook-loses-belgian-privacy-case-faces-fine-of-up-to-125-million-idUSKCN1G01LG
[19] Newcomb, Alyssa. "A timeline of Facebook's privacy issues – and its responses." NBC News. 2018. Paragraph 29. Accessed on 27/3/2018. https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651
[20] Cadwalladr, Carole and Graham-Harrison, Emma. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". The Guardian. 2018. Accessed on 24/3/2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
[21] Human Rights Watch. "Ethiopia: New Spate of Abusive Surveillance." *Human Rights Watch*. 2017. Par 3. https://www.hrw.org/news/2017/12/06/ethiopia-new-spate-abusive-surveillance
[22] Ibid. Par. 4, 7.

this type of targeted surveillance by governments to continue.[23] The goal of the UNHRC is to provide these stronger norms, incentives and regulations.

Another government that targets online privacy is China, which has strict censorship in place for entertainment, news and other media, including the "Great Firewall of China" technology to uphold this censorship.[24] People do not have access to Google, Facebook, Youtube, some international news-sources, and the use of virtual private networks (VPNs), which would have allowed people to access the Internet in a privacy, encrypted and anonymous fashion, is restricted.[25] The publicized goal of this censorship is to secure China's "cyber sovereignty, or protecting the country's internet from undue foreign influence".[26] However, the methods that are used to achieve this goal are stifling privacy and access to the internet. Currently, China has the "largest recorded number of imprisoned journalists and cyber-dissidents in the world," which is due to their mass surveillance program.[27] The combination of censorship, surveillance and the lack of privacy for citizens in order to protect national security presents another grey area.

Another example of a country that has restricted privacy online is Russia, which has introduced "legislation that limited the availability of [VPNs] and required users to disclose personal information before accessing messaging services," in order for the government to be able to link people's online presence to an identity.[28] While there are restrictions on surveillance, these are subject to interpretation by courts and the government, which allowed a citizen to be monitored and sentences for "extremist activities, namely antigovernment protests".[29] Currently, Russian law is unclear and inconsistent about what constitutes acceptable online speech and when mass surveillance is allowed.[30]

In Venezuela, there is evidence of spying operations targeting citizens and while Venezuelan law guarantees privacy of communications, "authorities have failed to apply these

---

[23] Marczak, B., G. Alexanders, S. McKune, J. Scott-Railton and R. Deibert. "Champing at the Cyberbit." *The Citizen Lab*. 2017. Par 117. https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/
[24] Bloomberg News. "The Great Firewall of China." 2017. Par 1. https://www.bloomberg.com/quicktake/great-firewall-of-china
[25] Bloomberg News. "The Great Firewall of China." 2017. Par 2. https://www.bloomberg.com/quicktake/great-firewall-of-china
[26] Ibid.
[27] Amnesty International. "Undermining freedom of expression in China." 2006. 16. https://www.amnesty.org/download/Documents/80000/pol300262006en.pdf
[28] Freedom House. "Freedom on the Net 2017: Russia." 2017, 1. https://freedomhouse.org/sites/default/files/FOTN%202017_Russia.pdf
[29] Ibid. 18.
[30] Human Rights Watch. "Online and on all fronts." 2017. Par 4. https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression

laws evenly".[31] As an explanation, Venezuelan authorities explained they are attempting to strengthen "national defense" and security, which includes increasing mass surveillance.[32] For similar reasons, Saudi Arabian mobile phone operators are now required to "fingerprint customers" to limit anonymous phone usage and link citizens to their online behaviour.[33] Additionally, authorities monitor websites, blogs, chat rooms, social media sites, emails and mobile phone text messages in the name of national security and "maintaining social order".[34]

These countries are examples of how widespread the use of online mass surveillance, spyware and intelligence gathering is on a global scale. The human right to privacy intersects with several other rights in many of these cases, including freedom of expression and national security. The grey area between these rights is where the UNHRC needs to examine its position and ensure the right to privacy in the digital age is defined and adhered to by the international community.

Past UN Actions

Figure 3: OHCHR. "UN experts raise concerns over 'landmark' Southeast Asian human rights declaration." *UN News* 2012. https://news.un.org/en/story/2012/11/425852

The United Nations has adopted multiple declarations, covenants, reports and resolutions addressing the issue of privacy in general and privacy in the digital age in particular.

i. 1948 – Adoption of the Universal Declaration of Human Rights by the United Nations General Assembly (hereafter UNGA)

The Universal Declaration of Human Rights was adopted in 1948 and set out a universal core of human rights and fundamental freedoms for the first time, including that of privacy. Article

[31] Freedom House. "Freedom on the Net: Venezuela." 2016. 19. https://freedomhouse.org/sites/default/files/FOTN%202017_Venezuela.pdf
[32] Ibid. 18.
[33] Freedom House. "Freedom on the Net: Saudi Arabia." 2016. 1. https://freedomhouse.org/sites/default/files/FOTN%202016%20Saudi%20Arabia.pdf
[34] Ibid. 12.

12 states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[35]

ii. 1966 – International Covenant on Civil and Political Rights

The General Assembly adopted the International Covenant on Civil and Political Rights, in which article 17 states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence".[36]

iii. 2007 – Founding of International Telecommunication Union's (ITU) Global Cybersecurity Agenda (hereafter GCA)

The ITU is the United Nations' specialized agency for information and communication technologies, which launched the GCA in 2007 as "a framework for international cooperation aimed at enhancing confidence and security in the information society".[37] Its five strategic pillars of deploying cybersecurity solutions are legal measures, technical & procedural measures, organizational structures, capacity building and international cooperation.[38] These five pillars were designed to structure a solution.

iv. 2012 – UNGA 20/8: Promotion, protection and enjoyment of human rights on the Internet

The Human Rights Council adopted a resolution that stated that "the same rights that people have offline must also be protected online, in particular freedom of expression".[39] It also recognized the increasing interest and importance of the exercise of human rights on the Internet.[40]

v. 2013 – UNGA 68/167: The right to privacy in the digital age

The General Assembly adopted a resolution that addressed the effect of technological advancements on privacy for the first time. It states that they enhance "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," in the

[35] The United Nations. Universal Declaration of Human Rights. 1948. Article 16.
[36] The United Nations General Assembly, International Covenant on Civil and Political Rights. 1966. Article 17. http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
[37] ITU, "Global Cybersecurity Agenda (GCA), paragraph 1. https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx
[38] ITU, "Global Cybersecurity Agenda (GCA), paragraph 3. https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx
[39] The United Nations General Assembly A/HRC/RES/20/8. 2012. https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement
[40] Ibid.

first address of the United Nations that links privacy to the Internet.[41] It requested the first report on this issue and asked for the examination of "the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale," the report of which was presented at the twenty-seventh session of the Human Rights Council.[42]

vi. 2014 – High Commissioner on Human Rights' Report on Right to Privacy in the Digital Age

As requested in resolution 68/167, the High Commissioner submitted 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".[43] It states that international human rights law provides "a clear and universal framework," but there is a lack of enforcement, safeguards, oversight and accountability in states.[44]

vii. 2014 – UNGA 28/39 Panel discussion on the right to privacy in the digital age

In 2014, the Human Rights Council held a panel discussion on the right to privacy in the digital age, which include the findings of the report by the High Commissioner as mentioned above.[45] The panellists concluded that while established frameworks continue to apply, "implementation of the law must be adapted to address the new reality" or technological advancements.[46] They asked for "sustained engagement of all stakeholders, including Governments, industry, civil society and international organizations" to ensure improved results.[47]

viii. 2017 – UNGA 34/7: The right to privacy in the digital age[48]

This resolution was adopted by the Human Rights Council. It recognized that more analysis and debate should be performed in order to promote the right to privacy.[49] It also calls all

[41] The United Nations General Assembly A/Res/68/167. 2014. http://undocs.org/A/RES/68/167
[42] Ibid.
[43] The United Nations Commissioner on Human Rights, Report on Right to Privacy in the Digital Age. 2014. https://ec.europa.eu/digital-single-market/en/news/right-privacy-digital-age-united-nations-report
[44] Ibid. 16.
[45] The United Nations High Commissioner for Human Rights, Summary of the panel discussion. 2014. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/28/39
[46] Ibid. 16.
[47] Ibid.
[48] The United Nations General Assembly A/HRC/RES/34/7. 2017. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/31/PDF/G1708631.pdf?OpenElement
[49] Ibid. 2.

states to adhere to and improve upon the implementation of laws and resolutions that have been passed before.[50]

These past UN actions have provided a framework and foundation for the discussion about the right to privacy in the digital age. The UNHRC's cause is to find a solution to improve the implementation and ensure engagement of all parties involved.

Possible solutions

The goal of the UNHRC is to recognize what facets of current international legislation and implementation need to be improved upon. The GCA has established five pillars to measure the "level of commitment of each nation in cybersecurity" as a structuring tool to advance possible solutions:

i. Legal Measures;

   Strategies for the development of a model for legislation that is interoperable and applicable globally

ii. Technical Measures;

   Strategies for the development of a global framework for security protocols, standards and software

iii. Organizational Measures;

   Strategies for the creation of organizational structures and policies on cybercrime, warning and incident response, generic and universal digital identity systems on a global scale

iv. Capacity Building;

   Strategies to facilitate human and institutional capacity building to obtain, improve and retain skills, knowledge, tools, equipment and other resources for the improvement of cybersecurity

v. National and International Cooperation.

   Proposals for a framework for international, dialogue, cooperation and coordination. [51]

These pillars can serve as a structuring tool to discover what improvements are necessary. Additionally, it is highly encouraged to include the content of these facets in a resolution, although it does not need to adhere to this format or wording.

[50] Ibid. 4.
[51] ITU, "Global Cybersecurity Agenda (GCA), paragraph 1. https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Conclusion

Addressing the right to privacy in the digital age is a challenging yet compelling issue for the international community and the UNHRC. The harsh reality for many people around the globe is a story of lack of clarity, lack of protection and lack of implementation for the protections that are in place for privacy. Thus, we need a new framework of privacy governance to cope with the implications of the new generation of online technologies, and to protect those who are not protected by means of international cooperation. The political will for solving this problem is often missing, since the grey area between the right to privacy and other rights is not made clear, and privacy is often not seen as a priority. That being said, delegates are encouraged to dig deep within the national, regional, and global scope to understand the intersection of the right to privacy with the existing political, economic, and social issues in order to encourage and inspire actual change.

Questions the resolution must answer

i. What is the definition of the right to privacy, and what would violate this right?
ii. Where is the limit of the implementation of the right to privacy in order to avoid violations of other human rights like the right to security?
iii. How will the resolution address all five pillars from the Global Cybersecurity Agenda to ensure international commitment (Legal Measures, Technical & Procedural Measures, Organizational Structures, Capacity Building and International Cooperation)?
iv. How can the international community collaborate with national governments and local authorities, as well as civil society and non-governmental organisations in addressing the right to privacy in the digital age?
v. How can a solution to violations of privacy be implemented?

Additional recommended reading/sources:

- UN archive on the right of Privacy: http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
- Global cybersecurity index 2017 as a measure of states' commitment to cybersecurity: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
- The Global Surveillance Industry: A report by Privacy International from 2016 that explains the current knowledge on international surveillance: https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf
- Mozilla's Internet Health Report shows the current international standings of privacy and security online, including the state of privacy laws in countries around the world: https://internethealthreport.org/v01/privacy-and-security/
- Freedom House's 2017 report on freedom online, with individual country's listing: https://freedomhouse.org/report/freedom-net/freedom-net-2017

Bibliography

Aladeokin, Adeyemi, Pavol Zavarsky and Neelam Memon, "Analysis and compliance evaluation of cookies-setting websites with privacy protection laws," *2017 Twelfth International Conference on Digital Information Management (ICDIM)*, Fukuoka, 2017, pp. 121-126. https://ieeexplore.ieee.org/abstract/document/8244646/

Amnesty International. "Undermining freedom of expression in China." 2006. 16. https://www.amnesty.org/download/Documents/80000/pol300262006en.pdf

Bloomberg News. "The Great Firewall of China." 2017. Par 1. https://www.bloomberg.com/quicktake/great-firewall-of-china

Cadwalladr, Carole and Graham-Harrison, Emma. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". The Guardian. 2018. Accessed on 24/3/2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Freedom House. "Freedom on the Net: Russia." 2017, 1. https://freedomhouse.org/sites/default/files/FOTN%202017_Russia.pdf

Freedom House. "Freedom on the Net: Saudi Arabia." 2016. 1. https://freedomhouse.org/sites/default/files/FOTN%202016%20Saudi%20Arabia.pdf

Freedom House. "Freedom on the Net: Venezuela." 2016. 19.

https://freedomhouse.org/sites/default/files/FOTN%202017_Venezuela.pdf

Global cybersecurity index 2017 as a measure of states' commitment to cybersecurity: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Greenwald, Glenn. "Revealed: how US and UK spy agencies defeat internet privacy and security." The Guardian. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Human Rights Watch. "Ethiopia: New Spate of Abusive Surveillance." *Human Rights Watch.* 2017. https://www.hrw.org/news/2017/12/06/ethiopia-new-spate-abusive-surveillance

Human Rights Watch. "Online and on all fronts." 2017. Par 4. https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression

ITU, "Global Cybersecurity Agenda (GCA). https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Lord, L. and D. Pannick (eds.). Human Rights Law and Practice. London, Butterworth, 2004.

Marczak, B., G. Alexanders, S. McKune, J. Scott-Railton and R. Deibert. "Champing at the Cyberbit." *The Citizen Lab*. 2017. Par 117. https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

Newcomb, Alyssa. "A timeline of Facebook's privacy issues – and its responses." NBC News. 2018. Paragraph 23. Accessed on 27/3/2018. https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651

Pew Research Center. "Global Opinions of U.S. Surveillance." 2014. http://www.pewglobal.org/2014/07/14/nsa-opinion/

Privacy International, "GLOBAL INTERNET LIBERTY CAMPAIGN PRIVACY AND HUMAN RIGHTS: An International Survey of Privacy Laws and Practice". Web.

Privacy International. "The Global Surveillance Industry." 2016. https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

Reuters Staff. "Facebook loses Belgian privacy case, faces fine of up to $125 million."

Reuters. 2018. Accessed on 27/3/2018. https://www.reuters.com/article/us-facebook-belgium/facebook-loses-belgian-privacy-case-faces-fine-of-up-to-125-million-idUSKCN1G01LG

Sprenger, P. “Sun on Privacy: ‘get over it’. Wired News. 1999. https://www.wired.com/1999/01/sun-on-privacy-get-over-it/

Statista, “Online Privacy – Statistics and Facts.” 2017. https://www.statista.com/topics/2476/online-privacy/

The Global Surveillance Industry: A report by Privacy International from 2016 that explains the current knowledge on international surveillance: https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

The United Nations Commissioner on Human Rights, Report on Right to Privacy in the Digital Age. 2014. https://ec.europa.eu/digital-single-market/en/news/right-privacy-digital-age-united-nations-report

The United Nations General Assembly A/HRC/RES/20/8. 2012. https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement

The United Nations General Assembly A/HRC/RES/26/13. 2014. http://hrlibrary.umn.edu/hrcouncil_res26-13.pdf

The United Nations General Assembly A/HRC/RES/28/16. 2015. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/068/78/PDF/G1506878.pdf?OpenElement

The United Nations General Assembly A/HRC/RES/32/13. 2016. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/156/90/PDF/G1615690.pdf?OpenElement

The United Nations General Assembly A/HRC/RES/34/7. 2017. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/31/PDF/G1708631.pdf?OpenElement

The United Nations General Assembly A/Res/68/167. 2014. http://undocs.org/A/RES/68/167

The United Nations General Assembly A/RES/69/166. 2015. http://undocs.org/A/RES/69/166

The United Nations General Assembly, International Covenant on Civil and Political Rights. 1966. http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

The United Nations High Commissioner for Human Rights, Summary of the panel

discussion. 2014.
http://www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/28/39
The United Nations High Commissioner.
http://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportPrivacy.aspx
The United Nations. A/69/397. 2014.
https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement
The United Nations. Universal Declaration of Human Rights. 1948. Print.