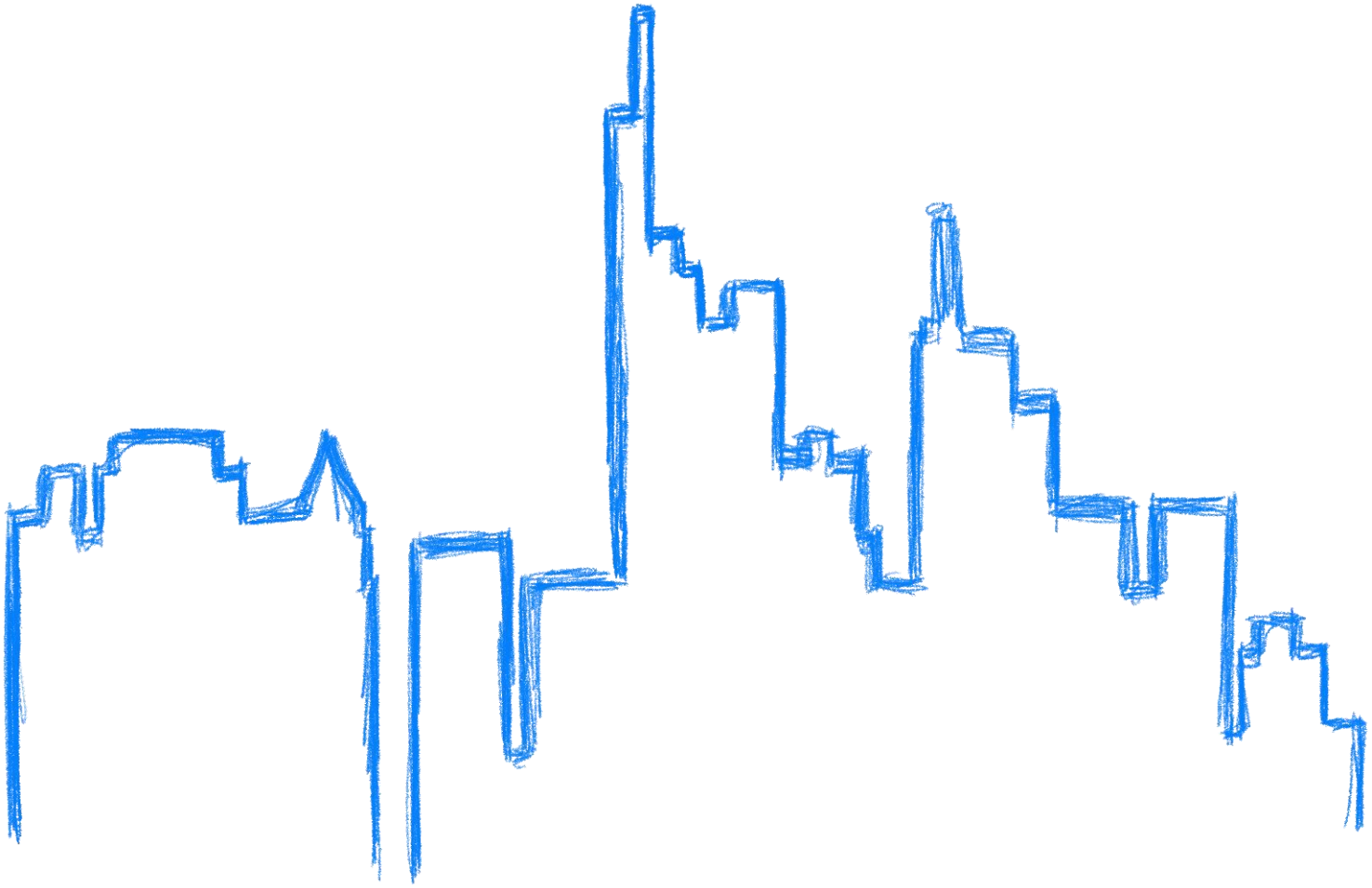
Main Model United Nations Conference

Frankfurt am Main, Germany

16th Session

5th to 7th of March 2021



Background Guide

Crisis Committee

Topic: The Right to Privacy in the Digital Age

Written By: Sarah Greifeld, Franziska Rosenbaum

Honourable delegates,

We would like to welcome you to the 2021 MainMUN conference, organised by students from Goethe-University Frankfurt am Main, Germany. We are looking forward to being your chairs in the Crisis committee . As your chairs, we would first like to introduce ourselves to you:

My name is Nathalie Ferko and I am currently writing my master thesis in political science at the Philipps-University of Marburg. Since the start of my MUN career in 2015, I gained a lot of experience as a delegate, board member, crisis member and Chair. This year I serve as the Faculty Advisor of MainMUN and stepped in as a Chair of the Crisis Committee. I would like to guide you, together with Sarah, through upcoming crisis to develop significant solutions.

I, Sarah, am currently working on my master's degree in American Studies in my third semester. I attended MainMUN as a delegate myself. Last year, I represented one of MainMUN's three Secretaries General. In the previous years, I chaired UN Women and the OSCE, so I am very excited to return to my position as Chair again this time (and maybe for the last time). I am looking forward to a great conference and fruitful debates with you all in March.

At MainMUN 2021, you will be simulating the Crisis committee, thus you will appear as a foreign minister of the country to which you were allocated. The topic of the Crisis committee this year will be:

The Right to Privacy in the Digital Age

In order to prepare efficiently for the conference, we recommend you do thorough research on the topic at hand. You may also want to become more familiar with your country's political positions so that the conference can be more enjoyable. Make sure that you are familiar with your respective country's policies and ideas in general.

We hope you find this background guide useful to introduce the topic of the Crisis committee. However, this does not, as previously mentioned, substitute further knowledge that can be

gained through individual research. We strongly encourage you to research your country's policies as well as possible partners for negotiations thoroughly. Furthermore, you should be aware of the bibliography used in the following. You may also find it useful to prepare notes and a position paper that can be submitted to us for the conference so that you are ready at any point during the debate.

We are looking forward to seeing you all online in the Crisis committee.

Sincerely,

Nathalie

Chair

Sarah

Chair

Table of Contents

1. Committee Description

During MainMUN 2021, you will be part of the Crisis committee. In this committee, the respective foreign ministers of the represented countries will participate in the debate. Since MainMUN is a Model United Nations with an interconnected approach, it means that most likely, the country delegation's head will participate in the Crisis committee. Furthermore, the interconnectivity allows the delegates to not only talk about the presented topic but also to interact with other delegates of their country delegation to establish a coherent policy that is to be applied throughout the conference. As the head of your country delegation, you can send instructions to other delegates of your country's delegation including the Security Council. As MainMUN 2021 and its outcome depends on the delegates' participation, the decisions and instructions are solely managed by them. Thus, the head delegates have a substantial influence on other committees and their work. Since the Crisis committee is off the regular structure of the United Nations, the delegates will address the world's current most important issues. However, the regular MainMUN Rules of Procedure for committees will be applied. In addition, the Crisis committee will apply further Rules of Procedure, which will be provided in the Crisis Handbook. These rules will explain how delegates can use and send directives so that specific actions during the conference may happen.Klicken Sie hier, um Text einzugeben. The topic of the MainMUN 2021 Crisis committee will be *the Right to Privacy in the Digital Age*. The Crisis committee will only focus on this one particular topic. However, news of important global issues, which need a debate within the framework of the Crisis committee, can arise any time. This means that delegates should prepare themselves to know and be able to apply their country's policies as they are representing the "real world" and you never know what will happen next. However, remember that MainMUN 2021 is a simulation and that the events, which happen outside of the conference do not interfere the procedures of the debates at the simulation. Due to the current pandemic, the Crisis committee will not use double delegations and each single delegate represents one country.

2. TOPIC: The Right to Privacy in the Digital Age

2.1 Introduction

The digital sphere has become part of our everyday life through the progress in information communication technology – including information-sharing and real-time communication. However, the increased use of technology blurs the lines between public and private spaces, which leads to both advantages and disadvantages. On the one hand, those technologies offer the opportunity for improvement in democratic participation as they increase the individual's access to information and facilitate the active participation in society. On the other hand, they have shown their vulnerability to interception and electronic surveillance.

By highlighting the importance of individual human rights, especially the right to privacy and the freedom of expression, the United Nations (UN) and several other institutions are deeply concerned about possible human rights violations and abuses by governments, companies and individuals via electronic surveillance and interception. The human right to privacy shall protect individuals from arbitrary or unlawful interference of their privacy and related spaces and it recognises the right of privacy as crucial for the realisation of the freedom of expression, which in turn is essential for every democratic and vibrant civil society. Within this context, it has become clear that the right to privacy and the freedom of expression need protection, whether online or offline in order to protect a free and democratic society.

2.2. International and Regional Legal Framework

Since the difficulties arising from privacy protection in the digital age are still relatively new, and although the right to digital privacy is granted through key international human rights documents, it lacks universal standards and definitions. Article 12 of the *Universal Declaration of Human Rights* (UDHR), which was adopted by the General Assembly in 1948, states 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."[1]

[1] UN General Assembly: *Universal Declaration of Human Rights*.

In addition, Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) (1966) uses the same terminology.[2] In contrast, Article 2 (1) of the treaty lines out that each member state is responsible for privacy protection, which complicates international work.[3] Many other international contexts, such as the *Convention on the Rights of Persons with Disabilities* (CRPD) (2006) and the *Convention on the Rights of the Child* (CRC) (1989), also line out the right to privacy specifically by stating that privacy is a fundamental right for disabled people and children. [4]

Not only has the importance of privacy protection been highlighted internationally, it also has been discussed on a regional level. As Article 8 of the 1950 *Convention for the Protection of Human Rights and Fundamental Freedoms* states: "[it] guarantees the right to respect for private life, family life, home and correspondence."[5] For European countries, the European Court of Human Rights strongly enforces the application of privacy rights since it employs a three-part test to current cases and rulings which depend on Article 8 of the European Convention on Human Rights (ECHR).[6] Furthermore, many of its current cases mirror the international framework as they deal with government surveillance of citizens and its degree of legality.[7] In addition to the European work on the topic of privacy protection, Article 11 of the *American Convention of Human Rights* and Article 17 of the *Arab Charter on Human Rights*,which was adopted in 1994, state similar guidelines to those published by the ECHR.[8] The African Union (AU) has not yet agreed on certain privacy guidelines. However, in 2014, its member states confirmed the *African Union Convention on Cyber Security and Personal*

[2] UN General Assembly: *International Covenant on Civil and Political Rights*.

[3] Ibid.

[4] UNICEF: *Using the human rights framework to promote the rights of children with disabilities*.

[5] Council of Europe: *Convention for the Protection of Human Rights and Fundamental Freedoms.*

[6] European Convention on Human Rights: *European Convention on Human Rights Art. 8*.

[7] Privacy International: *Legal Assessment of Communications Data Retention - A Violation of the European Convention on Human Rights.*

[8] League of Arab States: *Arab Charter on Human Rights*; Organization of American States: *American Convention on Human Rights "Pact of San Jose, Costa Rica".*

Data Protection.[9] Although this can be regarded as a significant change for the region as it entails the right to privacy, it seems likely that it will take a long time for it to be implemented.[10]

In addition to the UDHR and the ECHR, which indicate general privacy rights, there are also specific approaches to digital aspects of privacy protection which are at a more advanced stage than those of the AU. Particularly, the issue of the human right to privacy escalated during the 1970s, when computerised information was made available to the masses.[11] Due to this, some of the first countries to introduce legislation on the topic of data protection were France, Germany, Sweden and the United States of America.[12] The national legislations helped to initiate the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (1981).[13] The resulting data protection laws lined out the definition that personal data can be referred to "any information relating to an identified or identifiable individual."[14] The aforementioned laws provide secure treatment of personal data protection. Furthermore, in 2011, the Organisation for Economic Cooperation and Development (OECD) held its guidelines' 30th anniversary and re-examined the status of their formulated privacy guidelines with regards to current global issues.[15]

As much has been done to regulate one's right to privacy before the digital age, the discussions have more recently shifted towards regulations of a personal "online life". The Third Committee of the General Assembly (GA3) published *The Right to Privacy in the Digital Age* report in June 2014 addressed towards the Office of the United Nations High Commissioner for Human Rights (OHCHR), which focuses on "domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass

[9] Access Policy Team: *African Union adopts framework on cyber security and data protection.*

[10] Ibid.

[11] Privacy International: *Data Protection.*

[12] Ibid.

[13] Hunton & Williams LLP Tag Archives: *Council of Europe*.

[14] Council of Europe: *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (consolidated version).*

[15] OECD: *Current Developments in Privacy Frameworks - Towards Global Interoperability*.

scale".[16] The newly opened debate about the right to privacy in the digital sphere, as it became apparent that insufficient and outdated regulations, complicates the upholding of the human right. Further, the report helps to function as a guideline for future regulations on the topic.

2.3. The International Community

As of 2014, there are 5 resolutions that have been adopted by the GA3 on topics regarding digital human rights.[17] The most popular among those is the resolution A/RES/68/167 (2014), titled "the right to privacy in the digital age", which enforces guidelines about data collection and mass surveillance.[18]Furthermore, it outlined that illegal surveillance and data collection infringed people's rights to privacy in the digital sphere.[19] In 2019, the Human Rights Council agreed on resolution A/HRC/RES/42/15, in which the committee affirms that granted offline rights must be maintained online, too and that the rapid advancement of new technologies calls for further action on the topic as there could arise more infringements regarding the right to privacy. [20]

Additionally, the Human Rights Council (HRC) adopted a resolution in July 2012 which emphasises the "promotion, protection and enjoyment of human rights on the Internet, which affirms that the same rights that people have offline must also be protected online".[21] Furthermore, the worldwide corona pandemic, which began to affect member states in 2020 influences the right to privacy in the digital age, as there are new apps made to trace positive cases of COVID19. As these apps are supposed to notify those who were in potential contact with the virus, it could mean that cases of infringement to the right to privacy will rise. In order to fight the spread of COVID-19, the South Korean government used phone logs, card

[16] UN Human Rights Council: *The Right to Privacy in the Digital Age - Report of the Office of the United Nations High Commissioner for Human Rights.*

[17] Brown: *"Digital rights and the UN" - recent and upcoming UN resolutions.*

[18] Ibid.

[19] Ibid.

[20] UN Human Rights Council: *Resolution adopted by the Human Rights Council on 26 September 2019 (A/HRC/RES/42/15).*

[21]UN Human Rights Council: *The promotion, protection and enjoyment of human rights on the Internet.*

transaction records, and footage of surveillance cameras, leading to violations of the individuals' rights.[22]

Other important contributing factors to enforce human rights offline as well as online are intergovernmental organisations (IGOs) and non-governmental organisations (NGOs). One of the key actors is the *Freedom Online Coalition (FOC*).[23] This organisation helps to uphold privacy protection regulations with special regard to mass surveillance and has found itself in a leading position to advocate Internet freedom.[24]Another initiative that connects human rights activists with the civil society, government leaders and the private sector to discuss the importance of human rights in the digital age is *Internet Freedom Fellows*.[25]

Not only NGOs and IGOs influence the policies undertaken on the topic. The members of civil society can also promote their interests and influence the outcome of privacy right regulations through activism and awareness campaigns. An example for this is the statement that was published by civil society leaders to the Internet Governance Forum (IGF).[26] During the Eighth IGF in Indonesia in 2013, civil activists published a statement which opted for transparency, accountability and consistency.[27] Afterwards, multiple civil society organisations reac ted to that statement and responded to the report published by the HRC on state surveillance by publishing 13 principles for data protection. However, a collaboration between the HRC and civil actors has yet to be seen.[28] Although it may seem that these different actors may wish to pursue different results, they frequently interact with each other through various events and conferences held about the issue of digital privacy. By establishing its Internet Rights &

[22] TIME USA: *U.S. States Are Rolling Out COVID-19 Contact Tracing Apps. Months of Evidence From Europe Shows They're No Silver Bullet.*

[23] Human Rights Watch: *Joint Letter from Civil Society Organizations to Foreign Ministers of Freedom Online Coalition Member States.*

[24] Ibid.

[25] Internet Freedom Fellows: *Home.*

26 Freedom House: *Joint Statement of Civil Society Delegates to the 2013 Internet Governance Forum.*

27 Ibid.

28 Necessary and Proportionate: *International Principles on the Application of Human Rights to Communications Surveillance.*

Principles Coalition, the IGF provides the charter on "10 Internet Rights and Principles".[29] One of the rights listed is privacy and data protection and the charter explains that

> "everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal and disclosure".[30]

This reveals that the IGF is an important actor to the development of rights regarding digital privacy protection.

2.4. Online Activism and the Importance of Privacy: Understanding Privacy Violations

Due to the shift from offline to online in life as well as in matters of communication and action, political activism also moved to the spheres of the internet. One of the most remarkable examples might be the Arab Spring in 2011. The case of the Arab Spring in Tunisia between 2010 and 2011 illustrates the importance of social networks and the internet in the context of authoritarian or democratising systems.[31] The internet and social media both contributed to the intergroup collaboration and therefore circumvent one of the most pressing problems of collective action under authoritarianism, i.e. the lack of social interaction. It helped to exceed socio-economic and geographical boundaries and encouraged the cooperation between the urban middle class, the rural poor and the alienated intellectual elite.[32]

In sum, encouraging and supporting online activism in suppressing or democratising states emphasises the importance of the protection of data and the right to privacy. Laws, restricting

[29] Internet Rights & Principles Coalition: *Home*; Internet Rights & Principles Coalition: *10 Internet Rights & Principles.*

[30] Internet Rights & Principles Coalition: *10 Internet Rights & Principles.*

[31] Breuer, The Role of Social Media in Mobilizing Political Protest. Evidence from the Tunisian Revolution, 2012.

[32] Ibid.

state surveillance and the government's access to private technological activity also protect activists from being known by name which could have disastrous consequences to their life and security. Additionally, the right to privacy is also closely connected with the freedom of opinion and expression. In 2011, the UN Human Rights Council's (HRC) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, stated that the "inadequate protection of the right to privacy and data protection" and the "number of States introducing laws or modifying existing laws to increase their power to monitor Internet users' activities and content of communication without providing sufficient guarantees against abuse," eventually affects the people's ability and opportunity to freely express themselves without anonymity.[33]

Besides the implications illustrated by the foregone example, the blurring of governmental restrictions on private technology activity and illegal surveillance creates a fundamental distrust for current models of privacy protection.[34] Furthermore, it has a negative impact on the trust within the citizen-government relation when it comes to questions on data protection and it also influences the relationship between states when arguing about disagreements or differences in laws.[35] Around the collection of data that are done for the purpose of national security and criminal justice, there are several exceptions which are not clearly defined and therefore lead to legal loopholes in information collection An example would be the question of whose laws apply when considering the question of jurisdiction and territory.[36] In general, the ICCPR believes that "a State party must respect and ensure the rights laid down in the Covenant to anyone within the power of effective control of that State Party, even if not situated within the territory of the State Party."[37]

[33] UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/17/27)*, 2011.

[34] Schwartz, *Differing Privacy Regimes: A Mini-Poll on Mutual EU-U.S. Distrust*, 2014.

[35] European Digital Rights, *An Introduction to Data Protection*, 2013.

[36] Ibid.

[37] UN Human Rights Committee, *General Comment No. 31 [80]: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant (CCPR/C/21/Rev.1/Add. 1326)*, 2004.

2.5. The Private Sector and the Right to Privacy

The case of Google v. Spain has shown that the right to privacy does not only take effect within the relationship among governments and its citizens, but also in regard to the relation between citizens and private companies. In this case, the European Court ruled that every citizen has the right to ask search engines to remove any link containing private information.[38] As a reaction to Google's request, whether search engines have the same rules as other media outlets, the Court made its decision that the laws on privacy for media also apply to search engines.[39] In addition, the decision stated that the right to privacy outweighs the right to public access of information and financial interests. As already outlined in the foregone chapter, data collection and the right to privacy are essential issues for human rights in the private as well as in the governmental sector as technology continues to evolve.[40] The cases of several human rights defenders further reinforce the need for the protection of the right to privacy as they face harassment and threats because of the review of surveillance and personal information on groups or individuals.[41]

The obligation to and responsibility for privacy protection and the protection of the freedom of opinion and expression is not solely owned by the government but also by private companies which collect and proceed private information (e.g. Facebook, Google and Microsoft). Even if or especially because their mechanisms of data collection vary greatly in regard to their global location and the therefore applying laws.[42]

[38] EPIC, *The Right to Be Forgotten (Google V. Spain)*, 2017.

[39] Ibid.

[40] HRW, *Bold Step on Privacy and Digital Rights*, 2015.

[41] Ibid.

[42] Ibid.

2.6. Categories of Data in Need of Protection

Personal data and communication data are most prone to violations through data collection and mass surveillance.[43] With more accessible information and communication technologies, the protection of the human right to privacy is becoming more and more difficult which also stresses the importance of the right to deny access to personal data.[44] In this way, personal data is defined as "any piece of information or a set of information that can personally identify an individual or single them out as an individual",[45] like health records or an Internet Protocol (IP). The European Union gives us an example for a binding set of rules and implications on privacy protection with European Data Privacy Law and the European Union Data Privacy Direction. Within this scope, they provide a set of explicit directions as well as clarifications of the ambiguous ones for all Member States.[46] In order to protect the individual's privacy, those restrictions strive to anonymise a user's digital footprint by "removing or obscuring information from these electronic traces that would allow direct or indirect identification of a person."[47] However, this is only exemplary for the EU's efforts to protect personal data and communication.

Beyond the questions of data collection, the surveillance of mass communication is always subject to controversies. On the one hand, there are legitimate monitoring activities executed by the state in order to prevent terrorism and other serious threats. On the other hand, most states have agreements that prevent interceptions of digital and oral communication without judicial approval.[48] This kind of consideration also calls into question the balance between the rights to security and privacy.

---

[43] UN Human Rights Council, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37)*, 2013; Brown, *"Digital rights and the UN": recent and upcoming UN resolutions*, 2014.

[44] UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/23/40)*, 2013.

[45] European Digital Rights, *An Introduction to Data Protection*, 2013.

[46] 3 White & Case, *International Data Protection and Privacy Law*, 2009.

[47] European Digital Rights, *An Introduction to Data Protection*, 2013.

[48] White & Case, *International Data Protection and Privacy Law*, 2009.

2.7. Conclusion

The importance of fundamental human rights, like the right to privacy, is obvious, regardless of the context. Nonetheless, it became a quite special and important issue when people shifted parts of their life and communication from offline to online which created new spaces lacking definitions and protection. Due to future technical advancements and the therewith connected redefinition of privacy, the topic of the right to privacy will stay as important as or become even more important than it is right now. As states have the obligation and the responsibility to protect their citizens' right to privacy,[49] there is a need to evolve national and international law along technological advancements.

3. Possible Points of Discussion

- What does the right to privacy mean on an international and national level?
- How could the international community improve personal data protection, especially in the digital era?
- How can these laws be enforced without surveillance that interferes with the human right of privacy?
- Which actors besides member states should be included in the process of establishing new regulations and guidelines?

Further Research Questions

- How are your country's citizens affected by measures to protect privacy rights in a digital age?
- What measures has your country undertaken in order to implement the protection of privacy?
- How is the right to privacy and the right to freedom of opinion and expression handled by private companies in your country?

[49] UN General Assembly, *International Covenant on Civil and Political Rights*, 1966; Nyst, *Interference-Based Jurisdiction Over Violations of the Right to Privacy*, 2013.

4. Bibliography

(2020, October, 9). U.S. States Are Rolling Out COVID-19 Contact Tracing Apps. Months of Evidence From Europe Shows They‘re No Silver Bullet. Time USA. https://time.com/5898559/covid-19-contact-tracing-apps-privacy/

Access Policy Team, African Union adopts framework on cyber security and data protection, 2014.

Breuer, A. (2012). The Role of Social Media in Mobilizing Political Protest. Evidence from the Tunisian Revolution. German Development Institute. Discussion Paper 10/2012, Bonn.

Brown, D. (11 June 2014). “Digital rights and the UN”: recent and upcoming UN resolutions [Blog]. *Access.* Online: https://www.accessnow.org/blog/2014/06/11/Digital-rights-and-the-UN-recent-and upcoming-UN-resolutions

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No.11 and No. 14, 2010.

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (consolidated version), 1981.

Electronic Privacy Information Center. (2017). *The Right to Be Forgotten (Google v. Spain)* [Website]. Online: https://epic.org/privacy/right-to-be-forgotten/

European Convention on Human Rights, Art. 8 ECHR: Introduction, 2014. European Digital Rights. (2013). *An Introduction to Data Protection*. Online: http://www.edri.org/files/paper06_datap.pdf

Freedom House, Joint Statement of Civil Society Delegates to the 2013 Internet Governance Forum, 2013.

Human Rights Watch, Joint Letter from Civil Society Organizations to Foreign Ministers of Freedom Online Coalition Member States, 2014.

Human Rights Watch. (2015, July 8). *Bold Step on Privacy and Digital Rights*. Online: https://www.hrw.org/news/2015/07/08/bold-step-privacy-and-digital-rights

Hunton & Williams LLP, Tag Archives: Council of Europe, 2011.

Internet Freedom Fellows, Home, 2014.

Internet Rights & Principles Coalition, 10 Internet Rights & Principles, 2014.

Internet Rights & Principles Coalition, Home, 2013; Internet Rights & Principles Coalition, 10 Internet Rights & Principles, 2014.

League of Arab States, Arab Charter on Human Rights, 1994; Organization of American States. American Convention on Human Rights "Pact of San Jose, Costa Rica" (B-32), 1969.

Necessary and Proportionate, International Principles on the Application of Human Rights to Communications Surveillance, 2014

Nyst, C. (2013). Interference-Based Jurisdiction Over Violations of the Right to Privacy, EJIL: Talk! [Website]. European Journal of International Law. Online: http://www.ejiltalk.org/interference-basedjurisdiction-over-violations-of-the-right-to-privacy/

OECD, Current Developments in Privacy Frameworks: Towards Global Interoperability; Agenda, 2011.

Privacy International, Data Protection, 2014.

Privacy International, Report: Legal assessment of Communications Data Retention - A violation of the European Convention of Human Rights; Chapter: The right of privacy in the European Convention on Human Rights, 2012.

Schwartz, P. (2014). *Differing Privacy Regimes: A Mini-Poll on Mutual EU-U.S Distrust*. Online: http://paulschwartz.net/wpcontent/uploads/2014/07/Schwartz%20IAPP%20Blog%20MiniPoll%20(july%202014).pdf

UN General Assembly, International Covenant on Civil and Political Rights, 1966.

UN General Assembly, Universal Declaration of Human Rights (A/RES/217 A (III)), 1948, Preamble.

UN Human Rights Council, *Report of the Special Rapporteur on the promotion*

and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/17/27), 2011. Online: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

UN Human Rights Council, Resolution adopted by the Human Rights Council on 26 September 2019: The right to privacy in the digital age (A/HRC/RES/42/15), 2019.

UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet (A/HRC/RES/20/8), 2012.

UN Human Rights Council, The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37), 2014.

UNICEF, Using the human rights framework to promote the rights of children with disabilities: Discussion Paper, 2009.

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

United Nations, Human Rights Committee. (2004). *General Comment No. 31 [80]: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant (CCPR/C/21/Rev.1/Add. 1326)*. Online: http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsjYoiCfMKoIRv2FVaVzRkMjTnjRO%2bfud3cPVrcM9YR0iW6Txaxgp3f9kUFpWoq%2fhW%2fTpKi2tPhZsbEJw%2fGeZRASjdFuuJQRnbJEaUhby3WiQPl2mLFDe6ZSwMMvmQGVHA%3d%3d

United Nations, Human Rights Council. (2014). *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37)*. Online: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

White & Case. (2009). *International Data Protection and Privacy Law*. Online: http://www.whitecase.com/files/publication/367982f86dc9478eab2f5fdf2d96f84a/presentation/publicationattachment30c48c85a6c44c3784bd6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf