Human Rights Council

MCGSMUN 2018

LETTER FROM THE EXECUTIVE BOARD

Greetings Delegates!

We welcome you to the simulation of Human Rights Council at Mayo College Girls School Model United Nations Conference 2017 to be held on 20th to 23rd April, 2018. The committee shall be discussing 'Right to Privacy in the Digital Age' as its agenda.

There are a couple of things that we would like to communicate before you start your preparation. The agenda can be discussed on two equally important levels. First on the principal motivation behind any law that is or is advised to be in place and second, on the implementation, its practical impacts and the ground level impact on citizens. We would need you to research your country's stance on this agenda. This not only means that you study the policies your country has adopted but also the rationale behind that policy, why the country took a certain action, how it benefited your country, why other countries should consider adopting a similar policy and so on. Please try and understand thought the course of your research, what principle stance your country is aligned to and engage in discussion with other countries based on this stand.

If you have any queries, feel free to contact us.

Regards,

Parinay Gupta

parinaygupta24@gmail.com

+917042805393

A BRIEF ON UNITED NATIONS HUMAN RIGHTS COUNCIL

Responsibilities

The UN Human Rights Council is an intergovernmental organisation which works under the UN system. It is responsible for strengthening the promotion and protection of human rights around the globe and for addressing situations of human rights violations and make recommendations on them. It has the ability to discuss all thematic human rights issues and situations that require its attention throughout the year.

Creation

It is the successor of United Nations Commission of Human Rights. It was created by the United Nations General Assembly on 15 March 2006 by resolution 60/251. It has 47 members which are elected by the majority of UNGA through a secret ballot. Election takes place in every 3 years and members are not eligible for immediate re-election after two consecutive terms. The membership is based on equitable geographical distribution. The seats are distributed among the regional groups as follows:

- Group of African State: 13
- Group of Asian State: 13
- Group of Eastern Europe: 6
- Group of Latin America and Caribbean States: 8
- Group of Western European and Other States: 7

Principles

Human Rights Council promotes that the human rights should not be discriminated on the basis of race, colour, sex, language or religion, politics or other opinion, national or social origin, property, birth or other status. It believes that human rights are universal, indivisible, interrelated, inter-dependent and must be treated in a fair and equal manner.

Methodology

Human Rights Council enables dialogues between countries to strengthen the capacity of Member States to comply with their human rights obligations for the benefit of all human beings. It allows subsequent follow-up discussions to recommendations and their implementation. It strives to be transparent, fair, impartial and result-oriented.

Review Mechanism

Human Rights Council's work and functioning are reviewed by United Nations General Assembly in every five years after it had come into existence.

Complaint Procedure

On 18 June 2007, the Human Rights Council adopted resolution 5/1 entitled "Institution-Building of the United Nations Human Rights Council" by which a new complaint procedure was established to address consistent patterns of gross and

reliably attested violations of all human rights and all fundamental freedoms occurring in any part of the world and under any circumstances.

The complaint procedure addresses communications submitted by individuals, groups, or non-governmental organizations that claim to be victims of human rights violations or that have direct, reliable knowledge of such violations.

Special Procedures

The special procedures of the Human Rights Council are independent human rights experts with mandates to report and advise on human rights from a thematic or country-specific perspective. The system of Special Procedures is a central element of the United Nations human rights machinery and covers all human rights: civil, cultural, economic, political, and social. As of 27 March 2015 there are 41 thematic and 14 country mandates.

With the support of the Office of the United Nations High Commissioner for Human Rights (OHCHR), special procedures undertake country visits; act on individual cases and concerns of a broader, structural nature by sending communications to States and others in which they bring alleged violations or abuses to their attention; conduct thematic studies and convene expert consultations, contribute to the development of international human rights standards, engage in advocacy, raise public awareness, and provide advice for technical cooperation. Special procedures report annually to the Human Rights Council; the majority of the mandates also reports to the General Assembly. Their tasks are defined in the resolutions creating or extending their mandates.[1]

[1] http://www.ohchr.org/EN/HRBodies/HRC/Pages/AboutCouncil.aspx

CREDIBILITY OF SOURCES IN THE COUNCIL

We all understand that the internet today is flooded with information. We often encounter pieces of information or facts which are inaccurate or even fabricated. Many times we read news articles which are biased. This challenge, of determining which fact is true or not, sometimes becomes a bone of contention between different governments as well. Take for example India and Pakistan, which often accuse each other of initiating the violation of the ceasefire establish between them at the Line of Control (LoC). Thus, even at the international arena, veracity and acceptance of a fact by one or more government plays a major role in how an agenda is understood, deliberated or resolved. As it is likely that disputes may arise in the council related to the facts presented by various delegates, the Executive Board is sharing a list of sources which it will deem more credible than any other source. It means that if the Board has to decide which fact is true at a time of dispute resolution, then it may choose the fact from one of these sources over others.

But please note that as a representative of a country's government, you are free to look at all types of sources for your reference or preparation. However, it is advised that you cross-check facts from at least one of the following –

1. News Sources
    a. Reuters

It is an independent private news agency, which mostly covers international events of importance.

Website: www.reuters.com

    b. State operated News Agencies

In many countries the government itself partially or fully controls the media, and thus the subsequent flow of information. Hence, news reports from such outlets can be used by a participant to substantiate or refute a fact in context of that government's position on the agenda in the council. For examples,

    i. RIA Novosti (Russia)
    ii. IRNA (Iran)
    iii. Xinhua News Agency and CCTV (People's Republic of China)

2. Government Reports

These are reports which various organs, ministries, departments or affiliated agencies of a government release. They can be used in a similar way as the State Operated News Agencies reports. You may visit different governmental websites for the same. For Example,

    a. State Department of the United States of America

Website: www.state.gov

    b. Ministry of Foreign or External Affairs of various countries like India

Website: www.mea.gov.in

3. Permanent Representatives to the United Nations

This portal serves as a one-stop-shop for finding documents which reflect the activity of a country at United Nations or its affiliated bodies. The documents from these individual country websites also serve as a source for finding official statements by that country on various agendas. Do take note that the nature of websites varies a lot from country to country.

Source Link: www.un.org/en/members/

(Click on a particular country to get the website of the Office of its Permanent Representative.)

4. Other Multilateral or Inter-Governmental Organizations

These are international organisations which are apart from the United Nations. Usually one may find these organisation based around a specify region like South Asia, and a specific purpose such as trade, security or cooperation. Documents from the same can be deemed credible; most certainly for the countries which are a part of that organisation. For example,

    a. South Asian Association for Regional Cooperation (SAARC)

Website: www.saarc-sec.org

    b. The North Atlantic Treaty Organisation (NATO)

Website: www.nato.int/cps/en

5. United Nations and Affiliated Bodies

All reports or documents from the United Nations, its organs or affiliated bodies may be considered as a credible source of information.

Website: www.un.org

    a. Organs such as,

        i. UN Security Council

Website: www.un.org/Docs/sc/

        ii. UNGA

Website: www.un.org/en/ga/

    b. UN Affiliated bodies such,

        i. The International Atomic Energy Agency (IAEA)

Website: www.iaea.org

        ii. The World Bank (WB)

Website: www.worldbank.org

6. Documents from Treaty Based Bodies

These are bodies which are strictly formed for looking after the implementation of an international treaty or agreement. These agreements are pertinent to a specific theme; a document which various countries sign and agree upon. For example,

    a. The Antarctic Treaty System

Website: www.ats.aq/e/ats.htm'

b. The International Criminal Court

It is based on an agreement known as the Rome Statute.

Website: www.icc-cpi.int

INTRODUCTION

Digital communications technologies, such as the Internet, mobile smartphones and WIFI-enabled devices, have become part of everyday life. By improving access to information and real-time communication, innovations in communications technology have boosted freedom of expression, facilitated global debate and fostered democratic participation. By amplifying the voices of human rights defenders and providing them with new tools to document and expose abuses, these powerful technologies offer the promise of improved enjoyment of human rights. As contemporary life is played out ever more online, the Internet has become both universal and increasingly intimate.

In the digital era, communications technologies also facilitated Governments, companies and individuals to develop capabilities to conduct surveillance, interception and data collection. As noted by the Special Rapporteur on the right to freedom of expression and opinion, technological advancements have implied that the State's effectiveness in conducting surveillance is not limited any longer by scale or duration since the cost of technology declines and presence of data storages remove the financial or practical disincentives to conducting surveillance.

Consequently, the State has now the capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before thus making the global political, economic and social life increasingly reliant on the internet and hence vulnerable to mass surveillance, they may actually facilitate it.

As policies and practices that exploit this vulnerability of the digital communications technologies are exposed, deep concerns have been raised globally. Governmental mass surveillance is now emerging as a dangerous habit in jurisdictions rather than an exceptional measure as can be seen from examples of overt and covert digital surveillance around the world.

This can be seen where governments reportedly have threatened to ban the services of telecommunication and wireless equipment companies unless given direct access to communication traffic, tapped fibre-optic cables for surveillance purposes, and required companies systematically to disclose bulk information on customers and employees. Some have reportedly also made use of telecommunications networks to surveil and target political opposition members and/or political dissidents. Reports suggest that authorities in some States record all phone calls and retain them for analysis. With mass surveillance technologies entering the global market and even non-State groups reportedly developing sophisticated digital surveillance capabilities, the risk that digital surveillance will escape governmental controls is on the rise.

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

As mandated by resolution 68/167, the Office of the High Commissioner (OHCHR) will also submit the report to the Assembly at its sixty-ninth session.[2]

HISTORICAL ANALYSIS

Essentially, the timeline of mass surveillance can be separated into two distinct eras: pre-Snowden and post-Snowden. With Edward Snowden's leaks of the clandestine NSA and Five Eyes surveillance operations sparking significant international conversation, the world's attitude towards the ethics of mass surveillance saw a pivotal shift. However, despite the influence of Snowden, ignoring the roots of mass state-sponsored information interception would be a mistake; in a society where the fear of terrorism has reached new heights, it is of paramount importance to investigate history and study the dynamic between privacy and national security carefully.

Pre-Snowden Leaks

State surveillance first came to light in the 1970s, gaining the attention of legislators surrounding the NSA and its domestic spying practices. Despite this, mass surveillance did not receive tangible public attention until the revelation of the ECHELON network in 1980s and its subsequent affirmation in the 1990s. With the discovery of the ECHELON network, the public became cognizant of the NSA and its fellow UKUSA agreement members, or "Five Eyes" alliance. While the ECHELON network was initially revealed to be responsible solely for collecting the phone calls of a U.S. senator, by the late 1990s, ECHELON's true potential emerged. Notwithstanding ECHELON's reported ability to monitor up to 90% of all Internet traffic, the USA was, years later in 2001, still in denial of the network's existence.

In regards to mass surveillance, the 2000s were vital years that fuelled its advocates. Perhaps one of the most important terrorist attacks in history, the attack of 9/11 initiated a radically new outlook on national security. The United States signed the PATRIOT Act to substantially increase the surveillance and other counterterrorism efforts of the NSA, while the M15 began collecting bulk telephone communications data in the United Kingdom. Despite mass surveillance seeing more and more use in these years, there remained critics of both its effectiveness and ethics.

Formerly a high ranked intelligence official within the NSA, William Binney turned whistle-blower when he, along with colleagues and a house staffer, called upon the United States Defense Department to investigate Trailblazer, a NSA surveillance system that was designed to intercept data on communication networks such as the Internet. Binney publicly criticized the high funding of the project, saying that the United States was wasting "millions and millions" of dollars while also deeming the NSA's attempts to unravel the plot of 9/11 fruitless and wasteful.

2005 and 2006 saw two incidents of surveillance operations being reported in the news. In the former, The New York Times published an article with the headline, ""Bush Lets U.S. Spy on Callers Without Courts," while in the latter, USA Today revealed released a shocking report detailing the NSA's massive database from its domestic surveillance of tens of millions of Americans via their phones. Major telecom companies provided the NSA its information, but as revealed in 2007 by the CEO of Quest, complying with the NSA was sometimes necessary in order to be eligible for attractive business deals.

[2] http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc

It is interesting to note that despite the degree and nature of the 9/11 attacks in the US, public opinion on government surveillance has been largely unsupportive with the general population not being in support of public monitoring for the maintenance of national security.

Little Support for Phone Monitoring to Curb Terrorism

Percent who favor each as a measure to curb terrorism	Mid-Sept 2001 %	Aug 2002 %	Dec 2006 %	Aug 2011 %
Requiring that all citizens carry a national ID card at all times	70	59	57	57
Extra airport checks on passengers who appear to be of Middle-Eastern descent	--	59	57	53
Government monitoring credit card purchases	--	43	42	42
Government monitoring personal phone calls and emails	--	***33***	***34***	***29***

PEW RESEARCH CENTER Aug. 17-21, 2011.

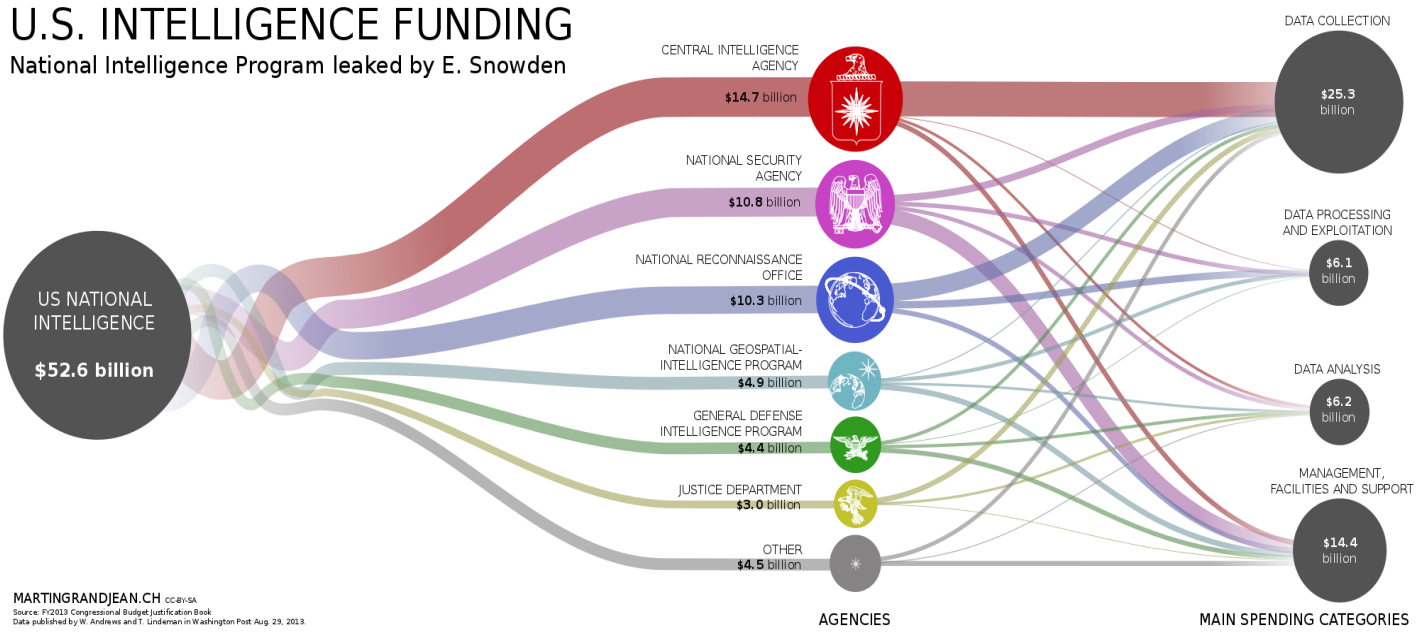
Edward Snowden and the NSA

An employee at the Central Intelligence Agency at the time in 2013, Edward James Snowden copied and publicly disclosed, without authorization, classified details from the United States National Security Agency. Originally published in two newspapers only, the leaks were soon covered by media outlets from around the world. From the leak, several global mass surveillance operations were exposed, including those of the NSA itself and its international partners in the Five Eyes Intelligence Agency (an intelligence alliance between Australia, Canada, New Zealand, the United Kingdom and the United States).

Not only were their own operations revealed, but the knowledge the agencies had of other international surveillance operations, such as those of Israel and Germany were also publicized. In the United States alone, it was revealed that with the aid of telecommunication companies and European governments, the NSA was conducting unwarranted surveillance operations including the unwarranted tapping of phones and Internet, thus compromising the privacy of the American people.

Using the same Internet surveillance programme, PRISM, Britain's electronic spy agency was also accused in Snowden's disclosures of collecting private information. While the American government charged Snowden with espionage and theft of government property shortly after, others have gone on to claim that he is a hero. Shortly after his conviction, Russia offered Snowden a temporary one year asylum within its orders and he was never again seen in the United States.

Irrespective of his label, Snowden shocked the world by releasing the clandestine operations of their own governments that undermined their inalienable individual rights to privacy, expression and association. The existence of mass surveillance came to the forefront of political affairs, along with individual and state level ramifications that will carry on into both the present and the future.[3]



[3] https://vmun.com/wp-content/uploads/VMUN-2017-UNHRC.pdf

THE RIGHT TO PRIVACY IN THE DIGITAL AGE: MEETING REPORT

Considering the recent revelations concerning mass surveillance, interception and data collection the Permanent Missions of Austria, Brazil, Germany, Liechtenstein, Mexico, Norway, and Switzerland hosted the expert seminar The Right to Privacy in the Digital Age in Geneva. The meeting was held to: examine the international human rights law framework in relation to the right to privacy, and identify challenges raised by modern communication technologies; foster understanding of how the right to privacy is implemented by governments, as well as the private sector and civil society; examine the extent to which domestic and extraterritorial surveillance may infringe an individual's right to privacy; and identify ways forward to ensure the protection and promotion of the right to privacy.

The seminar focused on best practice examples and lessons learned, as well as challenges at the national level. This snippet is a brief report of the meeting. This snippet does not express the views of the group as a whole nor should any points raised in it be associated with any individual or organization unless expressly stated.

The challenges posed by electronic surveillance and communications interception to the Right to privacy were identified and discussed and are listed as follows :

1. **Narrow interpretation of the right to privacy and broad interpretation of national security**

It was underscored during the meeting that national security and law enforcement are legitimate objectives for any state and that conducting surveillance operations, in compliance with human rights law, can be both necessary and effective means towards such objectives. However, some states have adopted an overly-restrictive interpretation of the right to privacy, while acing upon an overly broad interpretation of the legitimate scope of national security.

The decision to conduct surveillance activities must be based on balancing the interference with the right to privacy with the legitimate public interests which the authorities aim to protect. It was agreed that an independent judiciary is the best body to scrutinize surveillance applications and determine whether such a justification can be accepted. It was noted that transparency of the court's decision (e.g. how many cases, purpose) was essential. Concern was raised with regard to surveillance powers being used for purposes that are not considered justifiable, such as pursuing economic interests and gaining trade advantages.

2. **Non-existent, ambiguous or outdated national legislation**

Ensuring the protection of individuals against unlawful or arbitrary interference resulting from surveillance measures requires that effective national legal frameworks are in place. However in many jurisdictions, national legislation is non-existent, ambiguous or outdated and thus insufficient to protect against abuses in the light of surveillance techniques that technological advancements have enabled.

It was noted that states urgently need to review their national laws and practices, and ensure that clear and precise legislation is in place to protect the right to privacy, including in the realms of internet and telecommunications, and regulate communications surveillance by law enforcement and intelligence agencies. Legislation

should include anonymity protections for internet and telecommunications. The importance of data protection laws was highlighted and the states that do not have data protection laws in place were called upon urgently to enact such legislation. States should review their communications and data legislation on a regular basis to ensure that it keeps pace with technological advancements. Not only should the law be clear but also states' interpretation of it. Concern was raised with regard to legislation being interpreted by some states in an inconsistent manner leading to perverse applications of the law.

A further suggestion was that states should adopt export control legislation to ensure that companies cannot export surveillance technology to countries in which they will be used for human rights violations.

3. Proportionality and bulk collection of data

Participants noted that the bulk collection of data (i.e. mass surveillance) constitutes an interference with the right to privacy. Is such interference inherently disproportionate? Some held the view that non-targeted, indiscriminate mass surveillance of communications could never be proportionate and that any surveillance activity must always be targeted and justified on a case-by-case basis.

Jurisprudence from the European Court of Human Rights was relied on to argue that non-targeted surveillance undermines the rule of law. However others were of the opinion that the bulk collection of data may not necessarily be disproportionate (the example of security cameras was given to support this argument), but rather its use and storage might be. It was noted that, in any event, any surveillance method adopted must be in proportion to the legitimate aim and the least intrusive option available.

Lack of transparency was cited as a recurring obstacle to seeking judicial review of the proportionality of data surveillance. An assessment of whether surveillance is in fact proportionate to a legitimate aim requires transparency about (a) the scale of the interference with the right to privacy, (b) the purpose of the interference, and (c) the likelihood that this objective would be achieved.

4. Collection and meaning of metadata

It was noted that metadata can reveal very personal information and that distinguishing 'metadata' and 'content data' therefore is not meaningful, from a right to privacy perspective. The focus moved from the type of data that is being collected to: who is collecting the data; the extent of the information about the individual that can be obtained by analyzing the data; who is accessing the data; who is authorizing the data collection and on what grounds; and how long is the data being collected and stored for.

5. Lack of transparency and insufficient independent oversight

Although it is appreciated that some degree of secrecy may be necessary for national security and law enforcement objectives, current practice by some states demonstrates an unjustifiable lack of transparency with regard to surveillance practices. This lack of transparency is a serious obstacle to ensuring that surveillance practices are lawful, not arbitrary (i.e. are necessary and proportionate to meet a legitimate aim), ensuring accountability, access to a remedy, and the rule of law. Secret rules and secret interpretations, it was noted, do not have the necessary qualities of 'law', nor do rules that give authorities excessive discretion.

Businesses must also be more transparent about their role in communications surveillance, indeed a number of prominent internet and telecommunication businesses have been asking to be able to disclose more information about the access requests that they receive from governments. At a minimum business should be able to release quantitative information about such access requests.

Many states have not established effective, independent oversight mechanism to monitor surveillance practices. There must be judicial oversight, but equally courts must not be used to rubber stamp surveillance orders in the abstract. Courts must be able to review the application of the law in individual cases. Furthermore judicial oversight alone is not enough; rather all three branches of government should be engaged. Independent and adequately resourced parliamentary committees, review boards, data protection commissioners, independent advocates, and ombudspersons all have the potential to provide oversight of both state and business conduct.

Professional standards and codes of conduct for those that are tasked with monitoring data surveillance need to be developed. Such standards could be developed at a regional or potentially international level through consultations with stakeholders. Reporting requirements, applicable to both businesses and states, are also an integral part of maintaining transparency and allowing oversight.

The importance of whistleblower protection as a form of oversight was also emphasized.

6. Ex-post notification

Individuals need to be aware that they have been the subject of surveillance before they can access oversight mechanisms and/or a remedy. Although notification is not always feasible in legitimate, ongoing law enforcement and national security operations, there should always be ex-post notification.

To ensure that cases and operations do not remain open indefinitely, thus preventing ex-post notification, It was suggested that case files should be regularly reviewed and sunset clauses included within surveillance warrants.

7. Lack of accountability

Lack of transparency, oversight, and political will mean that ultimately there is little to no accountability in most states for arbitrary or illegal interference with the right to privacy by either the state itself or through the actions of a business entity, and therefore no remedy for victims. The strong EU law on access to data and the lack of implementation and enforcement of the law at national level was cited as an example of this.

8. Extraterritorial surveillance and jurisdiction

Since online and telecommunications do not necessary take a direct route, an email may circumvent the world and pass through the territory of many states before it is delivered to the recipient.

Furthermore the email may be stored on multiple servers spread around the world, thus a company may hold sensitive information about hundreds of thousands of people from all over the world and requests for access to that information may come from multiple states.

It was noted that this raises jurisdictional challenges, with questions over the extent to which a state's obligations under international human rights law may extend to extraterritorial communications surveillance. Reference was made to the position of the UN Human Rights Committee, which has said that states' obligations under the ICCPR extend not only to a state's territory, but to 'anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party.' Questions were raised over the extent to which this would apply to online communications.

In this regard, the universal nature of human rights was emphasized. Some suggested that, at a minimum, states' negative obligations (i.e. the obligation not to interfere unlawfully with the right to privacy) applies without any territorial limitation, while states' positive obligations (i.e. to protect the right to privacy from interference by third parties) only applies where a state has territorial control.

It was suggested that it is the action of the state, the causality between their actions and a resulting human rights violation that amounts to an exercise of jurisdiction. For example sending an agent onto foreign soil is an exercise of jurisdiction It was also suggested that if a state intercepts information passing through fiber-optic cables on its own territory this would also amount to jurisdiction.

The benefits and drawbacks of the Brazilian initiative, of requiring businesses to store Brazilian customers' data on servers within Brazil to try to prevent access to it by other states, were discussed.

There was disagreement on how local data storage would impact the development of the internet, particularly in poorer states. It was highlighted that local data storage requirements only limit the movements of communications from one point to another, communications can and will still be sent to third states.

There remain a number of practical challenges to ensuring access to remedies for an unlawful interference with one's right to privacy by a state acting extraterritorially. Moreover there is uncertainty over how to get redress for harm suffered as a result of one state's complicity in another state's unlawful infringement of the right to privacy, for example by hosting equipment within their territory which is then used for surveillance.

9. Targeting of foreign nationals

Concern was raised with regard to the practice of targeting foreign nationals as a means of circumventing protections offered to citizens under national legislation. Human rights treaties, including the ICCPR, require that the rights they protect be enjoyed equally by everyone without distinction or discrimination. Although distinctions based on nationality can sometimes legitimately be made by states for specific reasons, for example in relation to voting rights, the burden is on the state to justify that such a distinction is necessary for a legitimate aim and proportionate to that aim.

It was suggested that although a state can adopt stronger protections for its citizens, its duty to respect the minimum requirements of the universal right to privacy remains applicable to foreign nationals. Furthermore, it was highlighted that states have a positive duty to protect those within its jurisdiction from arbitrary and unlawful interference with their right to privacy, by other states and all diplomatic means should be taken to protect those within its jurisdiction from such interference.

10. The responsibility of business to respect the right to privacy

As we know from recent revelations, internet and telecommunications companies in some states are being obligated to hand over their customers' data, and if they refuse to do so they risk being shut down. In most cases these companies are prevented by law from disclosing that they have received such data access requests.

It was pointed out during the meeting that some businesses are systematically voluntarily handing over their customers' data. This practice was sternly criticized by participants. It was suggested that businesses should be encouraged to adopt policies that prohibit the voluntarily disclosure of customers' data. On the other hand, some businesses are pushing back and challenging the legitimacy of data access requests. It was asserted that businesses often receive informal requests, and when these are challenged (this could be as minor as asking for the source of the request) the requests are often dropped. As an example of best practice, Telenor was praised for insisting in all its contracts that all data access requests must be by court order.

A number of prominent businesses are pushing for states to be more transparent about the number and type of data access requests they are submitting and are calling for states to allow companies to publish the number and nature of state demands for customers' data and for governments to promptly disclose this information publicly.

The importance of the UN Guiding Principles on Business and Human Rights in ensuring that businesses are not complicit in human rights abuses was underscored. The Guiding Principles contain standards for businesses to adhere to in order to ensure their activities do not have a negative human rights impact; in this regard businesses should develop policies and constantly monitor their activities to ensure they are meeting these standards.

Ensuring that a business respects the Guiding Principles where there is no legislative oversight is a major challenge. It was noted during the meeting that states have a duty to protect those within their jurisdiction from human rights abuses by private actors, so long as this does not place an undue burden on the state. Included within this positive obligation is the duty to enact legislation regulating the conduct of business with regard to the right to privacy online. It was also highlighted that businesses have a responsibility not to put their employees in a situation where they would be acting unlawfully.

It was emphasized that in the main it is the private sector that develops and maintains our internet and telecommunications systems, and the private sector is an integral part of both the problem and the solution. Business must be actively engaged with by states and the international community to develop policies that ensure their conduct is in line with the Guiding Principles. It was agreed that businesses and states should seek to promote the use of strong encryption standards and that businesses should be using the strongest possible encryption codes available to them and states should be obligating internet and telecommunications providers to do so.

11. Freedom of the internet

The invaluable role the internet plays in upholding human rights and democratic participation in society was constantly highlighted during the experts meeting. The neutral and borderless nature of the internet was praised and calls made for its

protection. States should develop strong internet policies that are rooted in human rights norms. States should make efforts to guarantee access to the internet for all.[4]

[4] https://www.geneva-academy.ch/joomlatools-files/docman-files/ReportThe%20Right%20to%20Privacy%20in%20the%20Digital%20Age.pdf

MASS SURVEILLANCE

What is mass surveillance?

Mass surveillance is the subjection of a population or significant component of a group to indiscriminate monitoring. It involves a systematic interference with people's right to privacy. Any system that generates and collects data on individuals without attempting to limit the dataset to well-defined targeted individuals is a form of mass surveillance.

Under the methods that mass surveillance is now capable of being conducted, governments can capture virtually all aspects of our lives. Today it increasingly involves the generation, collection, and processing of information about large numbers of people, often without any regard to whether they are legally suspected of wrongdoing. At this scale, modern surveillance shifts the burden of proof, leads to an unaccountable increase in power, and has a chilling effect on individual action.

Is mass surveillance only a recent phenomenon?

While the mass surveillance of populations is currently on the rise, mainly due to rapid technological changes around the world, it has been used all throughout history.

One of the oldest forms of mass surveillance are national databases. These old administrative surveillance techniques include censuses registering the subjects of a kingdom, ID documenting individuals and tattoos marking them, and numbering and categorising humans.

The searchable nature of databases makes any data store a potential investigative tool and increases the potential of trawling. This is why national databases are supposed to be regulated carefully under law in democratic societies. Census databases collect detailed information on individuals in a country but should not be used to identify specific individuals or populations.

Identity schemes should be limited to very specific uses and not allow for discrimination or for abusive use of stop-and-identify powers. The increasing use of biometrics and the ability to query identity databases for matches and near-matches allows for fishing expeditions that increase the risk of abuse and re-use of the system for other purposes than for which it was designed.

Mass surveillance in public spaces became more commonplace with the deployment of closed-circuit television cameras (CCTV). Older systems collected vague images with limited capabilities of linking captured images to personal information. But now it is possible for people's movements to be tracked and stored for later analysis. Automated and real-time identification of large numbers of people is now undertaken, and the risk of further abuses is growing.

What are the latest forms of mass surveillance?

While databases and CCTV still exist and are in use, the most recent discussions around mass surveillance focus around the monitoring of communications, including what we do on our phones and our computers.

When it comes to spying on our phones, government authorities can now get access to data on everyone within a specific geographic area around a cell tower through bulk access to data held by mobile phone companies (often referred to as a 'cell tower dump'). We are also seeing an increase in the use of mobile surveillance tools that allow

authorities to monitor all communications and identify all devices within a localised area, for instance at a public protest by setting up fake mobile base stations.

Having started as mechanisms to administer and control large populations, then moving to capture 'public' actions, mass surveillance techniques are no longer restricted to public-facing activities. For instance, governments have passed laws mandating that all communications transactions are logged and retained by service providers to ensure that they are accessible to government authorities upon request. However, numerous courts have called this type of surveillance policy an interference with the right to privacy.

The technologies of mass surveillance are becoming more prevalent, and as resource limitations disappear, the capabilities for governments become endless. Now it is possible to monitor and retain an entire country's communications content, and directly access communications and metadata from undersea cable companies, telephone companies and internet service providers.

There are practically no limits on what governments can do with this broad access and the power that comes with unaccountable surveillance. For instance, in conducting fibre optic cable interception States can collect and read any the content of any unencrypted communication flowing through that cable – including phone calls, voice-over-IP calls, messages, emails, photos, and social networking activity. They can then apply a range of analysis techniques and filters to that information – from voice, text and facial recognition, to the mapping of networks and relationships, to behavioural analysis, to emotion detection.

Mass surveillance will be applied beyond communications surveillance. As we move towards 'smart' devices and cities, more and more of our activities will be collected and analysed. Smart meters report on our electricity usage, while smart cities track individuals and vehicles using cameras and sensors. Laws must keep up to date with these innovations that seek to monitor and profile us all. As the UN Office of the High Commissioner for Human Rights noted in 2014, "the technological platforms upon which global political, economic and social life are increasingly reliant are not only vulnerable to mass surveillance, they may actually facilitate it."

What's the problem with "collecting everything"?

Governments have been quick to attempt to colour the discourse around mass surveillance by rebranding their actions as “bulk collection” of communications, asserting that such collection in itself is a benign measure that does not offend privacy rights.

But what governments often do not point out is that collection of this information is where the interference to our privacy occurs. Mass surveillance programmes are premised on one fundamental objective – collect everything. Mine it, exploit it, extrapolate from it; look for correlations and patterns, suspicious thoughts or words, tenuous relationships or connections.

By starting from a position where everyone is a suspect, mass surveillance encourages the establishment of erroneous correlations and unfair suppositions. It enables individuals to be linked together on the basis of information that may be no more than a coincidence – a tube ride shared together, a website visited at the same time, a phone

connecting to the same cell tower – and conclusions to be drawn about the nature of those links.

Authorities can now have access to information concerning the entirety of an individual's life: everything they do, say, think, send, buy, imbibe, record, and obtain, everywhere they go and with whom, from when they wake up in the morning until when they go to sleep. Even the strongest of legal frameworks to govern mass surveillance with the strictest of independent oversight would leave room for abuse of power and misuse of information; for discriminatory attitudes and structural biases; and for human fallibility and malice.

The threat of being subject to such abuse, discrimination or error strikes results in changes in human behaviour, and consequently changes the way we act, speak, and communicate. This is the "chilling effect" of surveillance: the spectre of surveillance may limit, inhibit or dissuade someone's legitimate exercise of his or her rights.

These impacts include not only the violation of privacy rights, but extend to broader societal impacts on the ability to freely form and express ideas and opinions, to associate and organize, and to disagree with dominant political ideologies and demand change to the status quo.[5]

When is surveillance appropriate?

Many different groups define appropriate bounds for surveillance in different manners. One viewpoint that we have found interesting is that of M.I.T. professor Gary Marx, who argued that before implementing surveillance we should evaluate the proposed methods by asking a number of questions, which we enumerate below:

A. The Means

Harm: Does the technique cause unwarranted physical or psychological harm?

Boundary: Does the technique cross a personal boundary without permission (whether involving coercion or deception or a body, relational or spatial border)?

Trust: Does the technique violate assumptions that are made about how personal information will be treated such as no secret recordings?

Personal relationships: Is the tactic applied in a personal or impersonal setting?

Invalidity: Does the technique produce invalid results?

B. The Data Collection Context

Awareness: Are individuals aware that personal information is being collected, who seeks it and why?

Consent: Do individuals consent to the data collection?

Golden rule: Would those responsible for the surveillance (both the decision to apply it and its actual application) agree to be its subjects under the conditions in which they apply it to others?

Minimization: Does a principle of minimization apply?

[5] https://www.privacyinternational.org/node/52

Public decision-making: was the decision to use a tactic arrived at through some public discussion and decision making process?

Human review: Is there human review of machine generated results?

Right of inspection: Are people aware of the findings and how they were created?

Right to challenge and express a grievance: Are there procedures for challenging the results, or for entering alternative data or interpretations into the record?

Redress and sanctions: If the individual has been treated unfairly and procedures violated, are there appropriate means of redress? Are there means for discovering violations and penalties to encourage responsible surveillance behaviour?

Adequate data stewardship and protection: Can the security of the data be adequately protected?

Equality-inequality regarding availability and application: a) Is the means widely available or restricted to only the wealthiest, powerful or technologically sophisticated? b) Within a setting is the tactic broadly applied to all people or only to those less powerful or unable to resist c) If there are means of resisting the provision of personal information are these equally available, or restricted to the most privileged?

The symbolic meaning of a method: What does the use of a method communicate more generally?

The creation of unwanted precedents: Is it likely to create precedents that will lead to its application in undesirable ways?

Negative effects on surveillors and third parties: Are there negative effects on those beyond the subject?

C. Uses

Beneficiary: Does application of the tactic serve broad community goals, the goals of the object of surveillance or the personal goals of the data collector?

Proportionality: Is there an appropriate balance between the importance of the goal and the cost of the means?

Alternative means: Are other less costly means available?

Consequences of inaction: Where the means are very costly, what are the consequences of taking no surveillance action?

Protections: Are adequate steps taken to minimize costs and risk?

Appropriate vs. inappropriate goals: Are the goals of the data collection legitimate?

The goodness of fit between the means and the goal: Is there a clear link between the information collected and the goal sought?

Information used for original vs. other unrelated purposes: Is the personal information used for the reasons offered for its collection and for which consent may have been given and does the data stay with the original collector, or does it migrate elsewhere?

Failure to share secondary gains from the information: Is the personal data collected used for profit without permission from, or benefit to, the person who provided it?

Unfair disadvantage: is the information used in such a way as to cause unwarranted harm or disadvantage to its subject?[6]

[6] https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/ethics.html

RIGHT TO PRIVACY IN THE DIGITAL AGE: ISSUES TO CONSIDER

As recalled by the General Assembly in its resolution 68/167, international human rights law provides the universal framework against which any interference in individual privacy rights must be assessed. Article 12 of the Universal Declaration of Human Rights provides that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

The International Covenant on Civil and Political Rights, to date ratified by 167 States, provides in article 17 that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation". It further states that "everyone has the right to the protection of the law against such interference or attacks."

Other international human rights instruments contain similar provisions. Laws at the regional and national levels also reflect the right of all people to respect for their private and family life, home and correspondence or the right to recognition and respect for their dignity, personal integrity or reputation. In other words, there is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice.

While the mandate for the present report focused on the right to privacy, it should be underscored that other rights also may be affected by mass surveillance, the interception of digital communications and the collection of personal data. These include the rights to freedom of opinion and expression, and to seek, receive and impart information; to freedom of peaceful assembly and association; and to family life – rights all linked closely with the right to privacy and, increasingly, exercised through digital media. Other rights, such as the right to health, may also be affected by digital surveillance practices, for example where an individual refrains from seeking or communicating sensitive health-related information for fear that his or her anonymity may be compromised.

There are credible indications to suggest that digital technologies have been used to gather information that has then led to torture and other ill-treatment. Reports also indicate that metadata derived from electronic surveillance have been analysed to identify the location of targets for lethal drone strikes. Such strikes continue to raise grave concerns over compliance with international human rights law and humanitarian law, and accountability for any violations thereof. The linkages between mass surveillance and these other effects on human rights, while beyond the scope of the present report, merit further consideration.

A. The right to protection against arbitrary or unlawful interference with privacy, family, home or correspondence

Several contributions highlighted that, when conducted in compliance with the law, including international human rights law, surveillance of electronic communications data can be a necessary and effective measure for legitimate law enforcement or intelligence purposes. Revelations about digital mass surveillance have, however, raised questions around the extent to which such measures are consistent with international

legal standards and whether stronger surveillance safeguards are needed to protect against violations of human rights. Specifically, surveillance measures must not arbitrarily or unlawfully interfere with an individual's privacy, family, home or correspondence; Governments must take specific measures to ensure protection of the law against such interference.

A review of the various contributions received revealed that addressing these questions requires an assessment of what constitutes interference with privacy in the context of digital communications; of the meaning of "arbitrary and unlawful"; and of whose rights are protected under international human rights law, and where. The sections below address issues that were highlighted in various contributions.

1. Interference with privacy

International and regional human rights treaty bodies, courts, commissions and independent experts have all provided relevant guidance with regard to the scope and content of the right to privacy, including the meaning of "interference" with an individual's privacy. In its general comment No. 16, the Human Rights Committee underlined that compliance with article 17 of the International Covenant on Civil and Political Rights required that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. "Correspondence should be delivered to the addressee without interception and without being opened or otherwise read".

It has been suggested by some that the conveyance and exchange of personal information via electronic means is part of a conscious compromise through which individuals voluntarily surrender information about themselves and their relationships in return for digital access to goods, services and information. Serious questions arise, however, about the extent to which consumers are truly aware of what data they are sharing, how and with whom, and to what use they will be put.

According to one report, "a reality of big data is that once data is collected, it can be very difficult to keep anonymous. While there are promising research efforts underway to obscure personally identifiable information within large data sets, far more advanced efforts are presently in use to reidentify seemingly 'anonymous' data. Collective investment in the capability to fuse data is many times greater than investment in technologies that will enhance privacy." Furthermore, the authors of the report noted that "focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy", in part because "big data enables new, non-obvious, unexpectedly powerful uses of data".

In a similar vein, it has been suggested that the interception or collection of data about a communication, as opposed to the content of the communication, does not on its own constitute an interference with privacy. From the perspective of the right to privacy, this distinction is not persuasive. The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.

As the European Union Court of Justice recently observed, communications metadata "taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained." Recognition of this evolution

has prompted initiatives to reform existing policies and practices to ensure stronger protection of privacy.

It follows that any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful.

2. What is "arbitrary" or "unlawful"?

Interference with an individual's right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful. In its general comment No. 16, the Human Rights Committee explained that the term "unlawful" implied that no interference could take place "except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant". In other words, interference that is permissible under national law may nonetheless be "unlawful" if that national law is in conflict with the provisions of the International Covenant on Civil and Political Rights.

The expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of this concept, the Committee explained, "is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances".8 The Committee interpreted the concept of reasonableness to indicate that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case".

Unlike certain other provisions of the Covenant, article 17 does not include an explicit limitations clause. Guidance on the meaning of the qualifying words "arbitrary or unlawful" nonetheless can be drawn from the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights;10 the practice of the Human Rights Committee as reflected in its general comments, including Nos. 16, 27, 29, 34, and 31, findings on individual communications and concluding observations; regional and national case law; and the views of independent experts.

In its general comment No. 31 on the nature of the general legal obligation on States parties to the Covenant, for example, the Human Rights Committee provides that States parties must refrain from violation of the rights recognized by the Covenant, and that "any restrictions on any of [those] rights must be permissible under the relevant provisions of the Covenant. Where such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights." The Committee further underscored that "in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right."

These authoritative sources point to the overarching principles of legality, necessity and proportionality, the importance of which also was highlighted in many of the

contributions received. To begin with, any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available.16 Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.

Governments frequently justify digital communications surveillance programmes on the grounds of national security, including the risks posed by terrorism. Several contributions suggested that since digital communications technologies can be, and have been, used by individuals for criminal objectives (including recruitment for and the financing and commission of terrorist acts), the lawful, targeted surveillance of digital communication may constitute a necessary and effective measure for intelligence and/or law enforcement entities when conducted in compliance with international and domestic law. Surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a "legitimate aim" for purposes of an assessment from the viewpoint of article 17 of the Covenant. The degree of interference must, however, be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose.

In assessing the necessity of a measure, the Human Rights Committee, in its general comment No. 27, on article 12 of the International Covenant on Civil and Political Rights, stressed that that "the restrictions must not impair the essence of the right […]; the relation between right and restriction, between norm and exception, must not be reversed." The Committee further explained that "it is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them." Moreover, such measures must be proportionate: "the least intrusive instrument amongst those which might achieve the desired result".

Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.

Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of Governments on private sector actors to retain data "just in case" it is needed for government purposes. Mandatory third party data retention – a recurring feature of surveillance regimes in

many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.

One factor that must be considered in determining proportionality is what is done with bulk data and who may have access to them once collected. Many national frameworks lack "use limitations", instead allowing the collection of data for one legitimate aim, but subsequent use for others. The absence of effective use limitations has been exacerbated since 11 September 2001, with the line between criminal justice and protection of national security blurring significantly. The resulting sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating article 17 of the Covenant, because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another.

A review of national practice in government access to third-party data found "when combined with the greater ease with which national security and law enforcement gain access to private-sector data in the first place, the expanding freedom to share that information among agencies and use it for purposes beyond those for which it was collected represents a substantial weakening of traditional data protections." In several States, data-sharing regimes have been struck down by judicial review on such a basis. Others have suggested that such use limitations are a good practice to ensure the effective discharge of a State's obligations under article 17 of the Covenant, with meaningful sanctions for their violation.

B. Protection of the law

Paragraph 2 of article 17 of the International Covenant on Civil and Political Rights explicitly states that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy. This implies that any communications surveillance programme must be conducted on the basis of a publicly accessible law, which in turn must comply with the State's own constitutional regime and international human rights law. "Accessibility" requires not only that the law is published, but that it is sufficiently precise to enable the affected person to regulate his or her conduct, with foresight of the consequences that a given action may entail.

The State must ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse.

Consequently, secret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law". Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion; the scope and manner of exercise of authoritative discretion granted must be indicated (in the law itself, or in binding, published guidelines) with

reasonable clarity. A law that is accessible, but that does not have foreseeable effects, will not be adequate.

The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight. Several States also require that the legal framework be established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive – a requirement that helps to ensure that the legal framework is not only accessible to the public concerned after its adoption, but also during its development, in accordance with article 25 of the International Covenant on Civil and Political Rights.

The requirement of accessibility is also relevant when assessing the emerging practice of States to outsource surveillance tasks to others. There is credible information to suggest that some Governments systematically have routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. Reportedly, some Governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes.

Such practice arguably fails the test of lawfulness because, as some contributions for the present report pointed out, it makes the operation of the surveillance regime unforeseeable for those affected by it. It may undermine the essence of the right protected by article 17 of the International Covenant on Civil and Political Rights, and would therefore be prohibited by article 5 thereof. States have also failed to take effective measures to protect individuals within their jurisdiction against illegal surveillance practices by other States or business entities, in breach of their own human rights obligations.

C. Who is protected, and where?

The extraterritorial application of the International Covenant on Civil and Political Rights to digital surveillance was addressed in several of the contributions received. Whereas it is clear that certain aspects of the recently revealed surveillance programmes, for instance, will trigger the territorial obligations of States conducting surveillance, additional concerns have been expressed in relation to extraterritorial surveillance and the interception of communications.

Article 2 of the International Covenant on Civil and Political Rights requires each State party to respect and ensure to all persons within its territory and subject to its jurisdiction the rights recognized in the Covenant without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. The Human Rights Committee, in its general comment No. 31, affirmed that States parties are required by article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party." This extends to persons within their "authority".

The Human Rights Committee has been guided by the principle, as expressed even in its earliest jurisprudence, that a State may not avoid its international human rights

obligations by taking action outside its territory that it would be prohibited from taking "at home". This position is consonant with the views of the International Court of Justice, which has affirmed that the International Covenant on Civil and Political Rights is applicable in respect of acts done by a State "in the exercise of its jurisdiction outside its own territory", as well as articles 31 and 32 of the Vienna Convention on the Law of Treaties. The notions of "power" and "effective control" are indicators of whether a State is exercising "jurisdiction" or governmental powers, the abuse of which human rights protections are intended to constrain. A State cannot avoid its human rights responsibilities simply by refraining from bringing those powers within the bounds of law. To conclude otherwise would not only undermine the universality and essence of the rights protected by international human rights law, but may also create structural incentives for States to outsource surveillance to each other.

It follows that digital surveillance therefore may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protections must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violates another State's sovereignty.

This conclusion is equally important in the light of ongoing discussions on whether "foreigners" and "citizens" should have equal access to privacy protections within national security surveillance oversight regimes. Several legal regimes distinguish between the obligations owed to nationals or those within a State's territories, and non-nationals and those outside, or otherwise provide foreign or external communications with lower levels of protection. If there is uncertainty around whether data are foreign or domestic, intelligence agencies will often treat the data as foreign (since digital communications regularly pass "off-shore" at some point) and thus allow them to be collected and retained. The result is significantly weaker – or even non-existent – privacy protection for foreigners and non-citizens, as compared with those of citizens.

International human rights law is explicit with regard to the principle of nondiscrimination. Article 26 of the International Covenant on Civil and Political Rights provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law" and, further, that "in this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

These provisions are to be read together with articles 17, which provides that "no one shall be subjected to arbitrary interference with his privacy" and that "everyone has the right to the protection of the law against such interference or attacks" , as well as with article 2, paragraph 1. In this regard, the Human Rights Committee has underscored the importance of "measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the

nationality or location of individuals whose communications are under direct surveillance."

D. Procedural safeguards and effective oversight

Article 17, paragraph 2 of the International Covenant on Civil and Political Rights states that everyone has the right to the protection of the law against unlawful or arbitrary interference or attacks. The "protection of the law" must be given life through effective procedural safeguards, including effective, adequately resourced institutional arrangements. It is clear, however, that a lack of effective oversight has contributed to a lack of accountability for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Internal safeguards without independent, external monitoring in particular have proven ineffective against unlawful or arbitrary surveillance methods. While these safeguards may take a variety of forms, the involvement of all branches of government in the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law.

Judicial involvement that meets international standards relating to independence, impartiality and transparency can help to make it more likely that the overall statutory regime will meet the minimum standards that international human rights law requires. At the same time, judicial involvement in oversight should not be viewed as a panacea; in several countries, judicial warranting or review of the digital surveillance activities of intelligence and/or law enforcement agencies have amounted effectively to an exercise in rubber-stamping. Attention is therefore turning increasingly towards mixed models of administrative, judicial and parliamentary oversight, a point highlighted in several contributions for the present report.

There is particular interest in the creation of "public interest advocacy" positions within surveillance authorization processes. Given the growing role of third parties, such as Internet service providers, consideration may also need to be given to allowing such parties to participate in the authorization of surveillance measures affecting their interests or allowing them to challenge existing measures. The utility of independent advice, monitoring and/or review to help to ensure strict scrutiny of measures imposed under a statutory surveillance regime has been highlighted positively in relevant jurisprudence. Parliamentary committees also can play an important role; however, they may also lack the independence, resources or willingness to discover abuse, and may be subject to regulatory capture.

Jurisprudence at the regional level has emphasized the utility of an entirely independent oversight body, particularly to monitor the execution of approved surveillance measures. In 2009, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism suggested, therefore, that "there must be no secret surveillance system that is not under review of an independent oversight body and all interferences must be authorized through an independent body."

E. Right to an effective remedy

The International Covenant on Civil and Political Rights requires States parties to ensure that victims of violations of the Covenant have an effective remedy. Article 2, paragraph 3 (b) further specifies that States parties to the Covenant undertake "to ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other

competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy".

States must also ensure that the competent authorities enforce such remedies when granted. As the Human Rights Committee emphasized in its general comment No. 31, failure by a State party to investigate allegations of violations could in and of itself give rise to a separate breach of the Covenant. Moreover, cessation of an ongoing violation is an essential element of the right to an effective remedy.

Effective remedies for violations of privacy through digital surveillance can thus come in a variety of judicial, legislative or administrative forms. Effective remedies typically share certain characteristics. First, those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated. Notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to challenge such measures) thus become critical issues in determining access to effective remedy. States take different approaches to notification: while some require post facto notification of surveillance targets, once investigations have concluded, many regimes do not provide for notification.

Some may also formally require such notification in criminal cases; however, in practice, this stricture appears to be regularly ignored. There are also variable approaches at national level to the issue of an individual's standing to bring a judicial challenge. The European Court of Human Rights ruled that, while the existence of a surveillance regime might interfere with privacy, a claim that this created a rights violation was justiciable only where there was a "reasonable likelihood" that a person had actually been subjected to unlawful surveillance.

Second, effective remedies will involve prompt, thorough and impartial investigation of alleged violations. This may be provided through the provision of an "independent oversight body […] governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society." Third, for remedies to be effective, they must be capable of ending ongoing violations, for example, through ordering deletion of data or other reparation. Such remedial bodies must have "full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders". Fourth, where human rights violations rise to the level of gross violations, non-judicial remedies will not be adequate, as criminal prosecution will be required.

What role for business?

There is strong evidence of a growing reliance by Governments on the private sector to conduct and facilitate digital surveillance. On every continent, Governments have used both formal legal mechanisms and covert methods to gain access to content, as well as to metadata. This process is increasingly formalized: as telecommunications service provision shifts from the public sector to the private sector, there has been a "delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of 'self-regulation' or 'cooperation'". The enactment of statutory requirements for companies to make their networks "wiretap-ready" is a particular concern, not least because it creates an environment that facilitates sweeping surveillance measures.

There may be legitimate reasons for a State to require that an information and communications technology company provide user data; however, when a company

supplies data or user information to a State in response to a request that contravenes the right to privacy under international law, a company provides mass surveillance technology or equipment to States without adequate safeguards in place or where the information is otherwise used in violation of human rights, that company risks being complicit in or otherwise involved with human rights abuses. The Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011, provide a global standard for preventing and addressing adverse effects on human rights linked to business activity. The responsibility to respect human rights applies throughout a company's global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations.

Important multi-stakeholder efforts have been made to clarify the application of the Guiding Principles in the communications and information technology sector. Enterprises that provide content or Internet services, or supply the technology and equipment that make digital communications possible, for example, should adopt an explicit policy statement outlining their commitment to respect human rights throughout the company's activities. They should also have in place appropriate due diligence policies to identify, assess, prevent and mitigate any adverse impact. Companies should assess whether and how their terms of service, or their policies for gathering and sharing customer data, may result in an adverse impact on the human rights of their users.

Where enterprises are faced with government demands for access to data that do not comply with international human rights standards, they are expected to seek to honour the principles of human rights to the greatest extent possible, and to be able to demonstrate their ongoing efforts to do so. This can mean interpreting government demands as narrowly as possible, seeking clarification from a Government with regard to the scope and legal foundation for the demand, requiring a court order before meeting government requests for data, and communicating transparently with users about risks and compliance with government demands. There are positive examples of industry action in this regard, both by individual enterprises and through multi-stakeholder initiatives.

A central part of human rights due diligence as defined by the Guiding Principles is meaningful consultation with affected stakeholders. In the context of information and communications technology companies, this also includes ensuring that users have meaningful transparency about how their data are being gathered, stored, used and potentially shared with others, so that they are able to raise concerns and make informed decisions.

The Guiding Principles clarify that, where enterprises identify that they have caused or contributed to an adverse human rights impact, they have a responsibility to ensure remediation by providing remedy directly or cooperating with legitimate remedy processes. To enable remediation at the earliest possible stage, enterprises should establish operational-level grievance mechanisms. Such mechanisms may be particularly important in operating countries where rights are not adequately protected or where access to judicial and non-judicial remedies is lacking. In addition to such

elements as compensation and restitution, remedy should include information about which data have been shared with State authorities, and how.[7]

Is it not just the Government?

What is often overlooked in the debate over government surveillance of private communications is the widespread public concern over the amount of personal information businesses are collecting. In our 2012 political values survey, 64% said they were concerned that "the government is collecting too much information about people like me." Yet 74% expressed this concern about business corporations.

Concern that business corporations are collecting too much personal information crosses party lines. In addition, Republicans have become much more concerned about possible privacy intrusions by the government than they were during Bush's presidency (72% in 2012, 39% in 2007).

Privacy Concerns Not Restricted to Government

*Concerned that **business** is collecting too much personal information (% agree)*	2007 %	2012 %	Change
Total	74	74	0
Republican	58	72	+14
Democrat	80	74	-6
Independent	78	77	-1
*Concerned that **gov't** is collecting too much personal information (% agree)*			
Total	58	64	+6
Republican	39	72	+33
Democrat	66	60	-6
Independent	64	65	+1

PEW RESEARCH CENTER 2012 Values Survey. April 4-15, 2012.

[7] http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc

Additional Research Resources

The following excerpt has been taken from the Report to the 34th Session of the UN Human Rights Council – OHCHR. This document is the latest report of UNHRC Special Rapporteur which highlights the current challenges, the recent developments and a number of recommendations which the Rapporteur has made.

Recent developments and worrying trends in governmental surveillance

A. Governmental surveillance and privacy in the digital age – the Status quo

The current dialogue on governmental surveillance has been stimulated by people like Edward Snowden and those supporting him. Albeit controversial from a national perspective, it has to be acknowledged that the information he shared with the public about actual practices of national security services has sparked a necessary debate about what privacy means and should mean in the digital age. His famous quote "I do not want to live in a world where everything I do and say is recorded." has led to many crucial initiatives and actions.

The United Nations has followed up in several ways and called upon States in the resolution on privacy in the digital age "to establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data." Regional Human Rights Courts, such as the European Court of Human Rights in Strasbourg, have handed down judgements that establish clear and binding requirements that governments have to respect when establishing means to, and carrying out, surveillance.

The SRP mandate follows developments in government surveillance world-wide in a number of ways, including regular contact with a number of national and international CSOs. Many of the latter do an excellent job in bringing various matters of concern to the attention of the SRP as well as to national governments and the world in general. Without in any way detracting from the value of the work of other CSOs, the SRP would like to single out for attention the usefulness of the efforts of the following CSOs with whom the mandate collaborates in a variety of ways: ACLU, Access Now, Amnesty International, APC, Article19, Human Rights Watch, INCLO and Privacy International. It is extremely beneficial when relevant reports by these and other CSOs are published since the 10,300-word limit afforded to the SRP in formal reports does not permit him to include a narrative on, say, developments on surveillance as one may find in the report submitted to him by Privacy International in November 2016 and since published on the PI website. It is important to state that the SRP mandate share's PI's concerns about, and is independently following up related developments, in surveillance in Colombia, Estonia, France, Former Yugoslav Republic of Macedonia, (FYRM), Mexico, Morocco, New Zealand, Poland, Russia, Rwanda, South Africa, Sweden, Uganda, United Kingdom, United States of America, Venezuela and Zimbabwe. The SRP hereby invites the governments of these states to take note of the concerns expressed in

the PI submissions and very preferably respond publicly to such concerns and/or communicate directly to the SRP mandate as may be appropriate to the circumstances.

However, and deeply concerning, since the day the above-mentioned UN resolution has been passed and despite such judgments as mentioned in the preceding paragraph, the status of the right to privacy in the surveillance area of activity has not improved since the last SRP report. The states that reacted, started to work on and pass new laws on the subject that only, if at all, contain minor improvements in limited areas. In general, these laws have been drafted and rushed through the legislative process with political majorities to legitimize practices that should never have been implemented.

Recently, on the 21st of December 2016, the Court of Justice of the European Union delivered a very important and welcome judgment to remind the member states of the European Union of their duties to respect, promote and protect the human right to privacy and others in the digital age. With regards to legal obligations which require the retention of data in bulk by Telecommunication providers it stated: "The interference entailed by such legislation in the fundamental rights […] is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance […]." It also mentioned the negative potential consequences for the exercise of freedom of expression.

The judges further recognised "[…] while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight […]". Furthermore, the Court of Justice of the European Union made clear that the retention of traffic data must be the exception, not the rule. When there are concrete indications that such data must be kept for the fight against terrorism and serious crime, there must be limiting criteria in place such as precise geographical limitations. Additionally, the Court reiterates that people concerned need safeguards and remedies and there must be effective oversight mechanisms in place which involve checks and balances.

While privacy advocates understandably welcomed this judgement, the other dimensions of the decision were perhaps most usefully summed up by David Anderson, the UK's Independent Reviewer of Terrorism legislation "The judgment of the CJEU was thus a genuinely radical one. The proven utility of existing data retention powers, and the limitations now placed on those powers, is likely to mean that it will be of serious concern to law enforcement both in the UK and in other Member States. On the other side of the balance, not everyone will agree with the Court's view that these powers constitute a "particularly serious" interference with privacy rights, or that they are "likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance" (para 100). A more rigorous analysis of proportionality would have focussed on any actual harm that this useful power might be shown to have caused over its years of operation, and sought to avoid assertions based on theory or on informal predictions of popular feeling"

The SRP comes from a tradition deeply committed to evidence-based policy making which is why he shares Anderson's desire for a more rigorous analysis of proportionality. To date, the SRP has not yet been granted (in the UK at least) access to certain (sometimes classified) data which would confirm that the utility of bulk acquisition of data is both necessary and proportional to the risk. Indeed, the SRP welcomes the CJEU's judgement precisely because this evidence has not yet been made available that would persuade the SRP of the proportionality or necessity of laws regulating surveillance which permit bulk acquisition of all kinds of data including metadata as well as content.

It is important to draw attention to the cultural dimensions also noted by Anderson in this context:

"It must be acknowledged, however, that feelings on these matters do vary at least to some extent across Europe. Thus:

- The comments of the CJEU in relation to the seriousness of the interference with privacy find no real echo in the three parliamentary and expert reports which led to the introduction of the Investigatory Powers Bill, nor in the regular reports of the Interception of Communications Commissioner, the senior former Judge who conducts detailed oversight of this activity in the UK.

- But in the eastern part of Europe and in Germany, historic experience, coupled with a relative lack of exposure (until recently) to terrorism have induced greater circumspection. National data retention rules have proved controversial and were annulled even before Digital Rights Ireland in Bulgaria, Romania, Germany, Cyprus and the Czech Republic.

This may reflect what I have previously described as "marked and consistent differences of opinion between the European Courts and the British judges … which owe something at least to varying perceptions of police and security forces and to different (but equally legitimate) conclusions that are drawn from 20th century history in different parts of Europe" (A Question of Trust, 2.24)."

B. Challenges and worrying trends

Through various research activities of the mandate of the SRP and through other related research projects it has been found that the surveillance activities of LEAs and SIS are sometimes increasingly hard to distinguish from one another. While the activities of the one branch are typically directed towards the inside of a national territory and the activities of the latter towards foreign territory, the nature of trans-border dataflows and the technical needs required to interfere with them often result in the use of the same or very similar equipment in the digital age.

Increasingly, personal data ends up in the same "bucket" of data which can be used and re-used for all kinds of known and unknown purposes. This poses critical questions in areas such as requirements for gathering data, storing data, analysing data and ultimately erasing data. As a concrete example a recent study carried out by the Georgetown Centre on Privacy and Technology in the United States has found that "one in two American adults is in a law enforcement face recognition network." As the authors of the study put it: "We know very little about these systems. We don't know how they impact privacy and civil liberties. We don't know how they address accuracy

problems. And we don't know how any of these systems—local, state, or federal—affect racial and ethnic minorities."

These and similar insights lead to a couple of considerations: First, the nature of trans-border data flows and modern information technology requires a global approach to the protection and promotion of human rights and particularly the right to privacy. If the flow of information is to remain a global affair – with all of the substantial advantages that has brought and will continue to bring for humankind – there needs to be a consistent and trustworthy environment in which this happens. Such an environment cannot discriminate between people of different nations, origins, races, sex, age, abilities, confessions, etc. There needs to be a core of rights and values which is consistently respected, protected and promoted throughout the international community.

Secondly, the increasing importance of the exchange of information in the virtual space needs private, trustworthy and secure methods. Technologies such as encryption have already been discussed broadly by the Special Rapporteur on the right to privacy, and specifically in the first report to the General Assembly. Additionally, other Special Rapporteurs, such as the one on Freedom of Expression, have already carried out significant and welcome work in this area.

If LEAs and SIS are concerned about their inability not to intercept or read every message sent and received between anybody who uses modern information technology, they should not forget that we live in an age where information exchange happens through thousands of venues. Humans have started to share so much information through digital means that even if a couple of them are not accessible to the state, that does not mean that there are no other traces and venues to follow those people with bad intentions. Particularly, the vast amounts of metadata created by smartphones and connected devices, which often is as revealing as the actual content of communications, provides ample opportunities for the analysis of people's behaviour. On the other hand, if the state is capable of potentially interfering with every flow of information, even retroactively through bulk data retention and technologies such as "quick freeze", the right to privacy will simply not experience a full transition to the digital age.

It is to be welcomed that some countries and organizations have already started to increase their efforts to tackle these challenges. Particularly, the Council of Europe has contributed in this area with an initiative in the context of law enforcement in cloud computing environments. This is connected with the Cybercrime Convention and is aiming at developing a new legal tool.

Additionally, it is worrying that modern laws on surveillance increasingly allow for the creation, access and analysis of personal data without adequate authorisation and supervision. An adequate authorisation and supervision requirement should be in place when the measure "is first ordered, while it is being carried out, or after it has been terminated." While often "traditional" methods, such as the interception of phone calls and communications in general, are subject to judicial authorisation before the measure can be employed, other techniques such as the collection and analysis of metadata referring to protocols of internet browsing history or data originating from the use of smartphones (location, phone calls, usage of applications, etc.) are subject to much weaker safeguards. This is not justified since the latter categories of data are at least as

revealing of a person's individual activity as the actual content of a conversation. Hence, appropriate safeguards must also be in place for these measures.

While judicial authorisation of intrusive measures generally raises the degree of privacy protection, it also must be guaranteed that the judges themselves are independent and impartial in their decision-making process in individual cases. Furthermore, they must have the knowledge and facts necessary to consider the requests thoroughly and understand the potential implications of their decisions, particularly in terms of the technology to be employed, and the consequences of using that technology. Hence, states should provide the required training and resources necessary for judges to live up to this complicated task.

In principle, the same applies to the oversight of surveillance activities by specialized bodies of parliamentary assemblies. They need not only to have the relevant information to understand the activities of law enforcement agencies and security and information services, they also need to have adequate resources to comprehend and digest them.

In most countries this will be hard to achieve given the large volume of data involved. The authorities carrying out surveillance should take measures to guarantee internally that oversight practices are reviewed and controlled permanently and in detail. Oversight, particularly if carried out in the political sphere, should be able to focus on structural issues and be able to address the general direction of operations.

Another area which attracts a lot of attention is the international nature of oversight activities. There are particularly two dimensions to this phenomenon that require increased attention: First, it is of utmost importance that states respect the right to privacy, which is based on human dignity, on a global level. Surveillance activities, regardless of whether they are directed towards foreigners or citizens, must only be carried out in compliance with fundamental human rights such as privacy. Any national laws or international agreements disregarding this fact, must be considered outdated and incompatible with the universal nature of privacy and fundamental rights in the digital age.

III. First approaches to a more privacy-friendly oversight of government surveillance

A. Comprehensive overview of approaches and themes

Research and exchange with several national authorities, civil society and corporations from different global regions, especially within IIOF2016, have shown the emergence of several themes in the area of governmental surveillance. These are:

- A need for internationalization and standardization of terms and language used;
- A need for a confidential and open dialogue to better understand national systems, their similarities and differences;
- The promotion and protection of Fundamental Human Rights in relation to the methods used;
- Safeguards and Remedies – preferably on an international level;
- Accountability and transparency;
- Collection and discussion of good and bad practices;
- A more evolved discussion on how to structure oversight of governmental surveillance;

- Answers to the question on how to engage with the public;
- The need to be less secretive and more proactive in explaining the work of secret services and law enforcement authorities when carrying out surveillance;
- A need for more fora to make progress on the subject.

Questions to Consider

- ✓ What kind of data should be private? What kind of data should the general public have access to? Governments?
- ✓ How can we weigh individual privacy with national security concerns? At what point does surveillance become an invasion?
- ✓ Why has little action been taking so far? What are the preventing factors?
- ✓ How can international action be taken in a way that is adaptable and fluid as technology develops and private data changes? What kind of private data did not exist 50 years ago?
- ✓ What domestic laws does your country have regarding data privacy? To what extent does your nation enforce said laws? What nations share similar laws?
- ✓ How has your state responded to recent international actions?
- ✓ What kinds of international actions might be effective? What are the potential factors that might prevent such an action?
- ✓ What organizations or companies have a vested interest in action on this topic? Who might suffer?