The Right to Privacy in the Digital Age: Meeting Report

In light of the recent revelations regarding mass surveillance, interception and data collection the Permanent Missions of Austria, Brazil, Germany, Liechtenstein, Mexico, Norway, and Switzerland hosted the one and a half day expert seminar **The Right to Privacy in the Digital Age** in Geneva on 24-25 February 2014. 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 document is a report of the meeting. This report does not express the views of the group as a whole nor should any points raised in it be associated with any individual or organisation unless expressly stated.

The New Digital Age

The development of new information technology has improved the ability to communicate and share information with others, thus enhancing freedom of expression and democratic participation. However, these technological developments have also made it possible for electronic surveillance and communications interception to be carried out on a large scale and with relative ease. As the United Nations High Commissioner for Human Rights cautioned in her opening remarks to the seminar, such practice 'threatens individual rights – including to privacy and to freedom of expression and association – and inhibits the free functioning of a vibrant civil society.' Furthermore, arbitrary communications surveillance poses a threat to anonymity of communications and in turn human rights defenders, whistleblowers and investigative journalism – all of which are important elements of a free and democratic society.

The Right to Privacy

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides that no one shall be subjected to an arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation, and that everyone has the right to the protection of the law against such interference or attacks.

Participants noted that the right to privacy is not simply a right to be 'left alone', but rather its essence concerns an individual's autonomous development in the community, and the ability to communicate with others in order to fulfil their personal development. It was underscored that the right to privacy is interlinked with the right to freedom of expression: the two are mutually dependent upon one another and both facilitate the ability of individuals to participate in free and democratic societies. The right to a privacy is a liberty right, protecting an individual's choice what to share and with whom.

Participants noted the affirmation, by the General Assembly and the Human Rights Council, that the right to privacy applies to online activity and communications, and that the surveillance, interception, collection and storage of online activity and communications does engage the right to privacy. As General Assembly resolution 68/167 recalls, international human rights law provides the universal framework against which any interference in individual privacy rights must be assessed. While the right to privacy is not absolute, any limitation to it must: be provided by law (meaning the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorised to conduct data surveillance and under what circumstances); be necessary for reaching a legitimate aim; and be proportionate (meaning the surveillance activity must be in proportion to the aim and the least intrusive option available). Moreover the limitation placed on the right (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. There is a burden on the authorities that sought to limit the right to show that the limitation is really connected to the 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 on discrimination. Where the limitation does not meet these criteria the limitation is unlawful and the interference with the right to privacy is arbitrary. The work of the UN Human Rights Committee, for example in its General Comments 27, 29, 31 and 34, was highlighted as an important source for guidance with regard to permissible limitations.

A number of challenges posed by electronic surveillance and communications interception to the right to privacy were identified and discussed during the meeting. These are as follows.

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.

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 note 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.

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. This raised a question over whether such interference was 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.[1] 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.

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 should move 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 authorising the data collection and on what grounds; and how long is the data being collected and stored for.

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.

[1] *Leander v. Sweden,* (1987) 9 EHRR 433; *Amann v. Switzerland* (2000)30 EHRR 843; and *S and Marper v. UK* (2009) 48 EHRR 50.

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.

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, on-going 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.

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.

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.

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.

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.[2]

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

[2] Global Governance Surveillance Reform, Principle Three.

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.

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.

Summary of conclusions

In sum, the overall conclusions of the meeting were:

- States urgently need to undertake a review their national law and where necessary adopt clear and precise legislation that both protects the right to privacy, including in internet and telecommunications, and regulates communications surveillance by law enforcement and intelligence agencies. Legislation should include anonymity protection for internet and telecommunications. State should also enact data protection laws. States should review their communications and data legislation on a regular basis to ensure that it keeps pace with technological advancements.
- Current practice by states demonstrates an unjustifiable lack of transparency. At a minimum states should be releasing quantitative information about access requests. Those individuals that have been the subject of an surveillance operation must be given ex-post notification
- The decision to conduct data surveillance activities must be based on limiting privacy through a justified and proscribed public interest. The surveillance method used must be the least intrusive method available.
- An independent judiciary should scrutinize surveillance requests.

- All three branches of government should be engaged in the oversight of surveillance activities 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.
- The focus should move from the type of data that is being collected to: who is collecting the data; who is accessing the data; who is authorising the data collection and on what grounds; and how long is the data being collected and stored for.
- Caution should be exercised when we trust or accept safeguards of safe storage and anonymisation, as all data storage is capable of being hacked and anonymisation can be undone.
- Businesses should be using the strongest possible encryption codes available to them and states should be obligating internet and telecommunications providers to do so.
- The neutral and universal nature of the internet must be protected.

Ways forward

Several specific options for ways forward were discussed, none of which are mutually exclusive:

Special Rapporteur

Some noted that the establishment by the UN Human Rights Council of a new mandate for a Special Rapporteur on the right to privacy would be a welcome development. However, concern was raised over whether or not this is a realistic option, at least in the immediate future given the resistance by many states to the creation of new mandates, in particular in light of resource constraints. The suggestion was made that one of the 'less pressing' mandates could be suspended and resources diverted to fulfilling a new mandate on the right to privacy.

Joint Initiative by the relevant special procedures mandates

Another suggestion would be to encourage those Special Rapporteurs whose mandates are concerned with privacy and national security practices (such as the UN Special Rapporteurs on the right to freedom of opinion and expression, and on human rights and fundamental freedoms while countering terrorism) to engage in a joint initiative, for example to clarify the applicable legal standards and principles, and/or develop guidelines or best practices on ensuring respect for the right to privacy in the digital age.

A Commission to conduct follow-up to the report of the High Commissioner for Human Rights

It was further suggested that the Human Rights Council could establish a time-bound commission to conduct follow-up to the report of the High Commissioner on the right to privacy in the digital age. Such a commission would ensure that the Human Rights Council maintains a focus on the issue and could be used to engage all stakeholders.

New Optional Protocol to the ICCPR

Some have suggested the development of an Optional Protocol to the ICCPR on the right to privacy in order to affirm and further elaborate on the right to privacy. However the disadvantages include that it may be difficult to arrive at an agreed text; it may invite an argument that existing legal standards do not apply to digital communications; it may lower existing standards; and those states that do not ratify it would remain free to argue they are not bound by the standards elaborated in the protocol.

It was felt that as the existing legal framework covers the right to privacy in the digital age, efforts should concentrate instead on ensuring this existing body of law is implemented.

New Human Rights Committee General Comment

Many have noted that a new General Comment on Article 17 of the ICCPR would be welcome. However as the agenda of the Human Rights Committee is already very full it is understood that this may not happen in the immediate future; in the meantime General Comment 16 (1988) is still relevant.

Inter-state complaint to the Human Rights Committee

Those states that have made a declaration under article 41 of the ICCPR could make an inter-state complaint about one of the so-called 'five-eyes' states (all of which have made an Article 41 declaration). This would be a politically risky move.

Working Group on the issue of human rights and transnational corporations and other business enterprises

The UN Working Group on Business and Human Rights may be a useful channel for engaging with business on issues related to the right to privacy in the digital age. The 2014 Forum on Business and Human Rights could also be used to facilitate multi-stakeholder dialogue on this issue.

Promotion of voluntary commitments

Businesses should be encouraged and supported to adopt voluntary commitments and standards, similar to the Guiding Principles, on ensuring the protection of the right to privacy on the internet and in telecommunication.

Seek an Advisory Opinion from the International Court of Justice

Whether or not it would be beneficial to seek an Advisory Opinion was discussed. It was agreed that this would be risky move politically, could potentially backfire, and the question asked would have to be carefully considered and clearly drafted. One option put forward was to ask a general question, such as clarification of the word 'arbitrary' in Art 17 ICCPR, with the aim of drawing the international community's attention to the issue. Another was to ask a question solely with regard to the threshold applicability questions with respect to extraterritorial surveillance.

However many were of the view that in the near term it would be premature to seek an Advisory Opinion from the ICJ and this option should be reconsidered once more work has been done by special procedures or any ad hoc bodies to be established and once we have more jurisprudence from ECtHR and the Human Rights Committee.

Relevant reports, legislation and initiatives

The International Principles for the Application of Human Rights to Communications Surveillance

The principles are the outcome of a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology. The principles are designed to provide civil society groups, industry, states and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights.

Global Governance and Surveillance Reform; Five Principles

The five principles were developed by AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo who are calling on states to endorse and enact the principles which relate to: 1) limiting governments authority to collect users' information; 2) Oversight and accountability; 3) Transparency about government demands; 4) Respecting the free flow of information; 5) Avoiding Conflicts Among Governments

UN human rights system

- Report of the UN Special Rapporteur on the Right to Freedom of Opinion and Expression, A/HRC/23/40
- Report of the UN Special Rapporteur on human rights and fundamental freedoms while countering terrorism, A/HRC/13/37
- General Assembly Resolution 68/167

European Declarations Conventions

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). The Data Protection Convention is open to European as well as non-European states. The Convention is currently undergoing a consultation process to modernise it.
- Convention on Cybercrime (ET S - No. 185) Open to non-Council of Europe states.
- Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies

Pending cases at the ECtHR

- *Big Brother Watch and others v. UK* (fast tracked, communicated on 9 January 2014)
- *Centrum for Rttvisa v.* Sweden (lodged 14 July 2008)

The Global Network Initiative (GNI)

GNI brings together companies with civil society organizations, investors, and academics to forge a common approach to protecting and advancing free expression and privacy online.
The GNI Principles provide focused guidance on how ICT companies can respond to government requests implicating privacy in ways that respect the rights of users, backed by the independent assessment of company implementation.