Expert workshop with the purpose of identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy in the digital age, including the responsibility of business enterprises in this regard

19 & 20 February 2018, Palais Wilson, Ground Floor, Geneva

CONCEPT NOTE

I. INTRODUCTION

1. In operative paragraph 10 of resolution 34/7, the Human Rights Council requested the Office of the United Nations High Commissioner for Human Rights "to organize, before the thirty-seventh session of the Human Rights Council, an expert workshop with the purpose of identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy in the digital age, including the responsibility of business enterprises in this regard, to prepare a report thereon and to submit it to the Council at its thirty-ninth session."

II. BACKGROUND

2. The right to privacy is recognized, inter alia, in Articles 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Political and Civil Rights. It is also an essential requirement for the realization of other human rights, including the right to freedom of opinion and expression. It is a core foundation of democracies and its respect constitutes an important element for a thriving civil society. In view of technological developments, in particular in the fields of communication and information technology, ensuring the protection and promotion of the right to privacy in the context of modern communications and information technology raises specific challenges.

3. Innovations in technology have increased the possibilities for the free exchange and access to information, creating new ways of exercising the right to freedom of expression and information. At the same time, these innovations have increased the

capacity of States and non-State actors to conduct surveillance, decryption and mass data collection and use, which may have an impact on individuals' right to privacy.

4. The right to privacy in recent years has attracted increasing attention from the United Nations General Assembly and human rights mechanisms, in particular with regard to surveillance policies and practices of many governments across the globe. In 2013, the General Assembly adopted resolution 68/167, in which it expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights. The General Assembly affirmed that the rights held by people offline must also be protected online, and called upon all States to respect and protect the right to privacy in digital communication. In line with the request of the General Assembly as reflected in that resolution, the High Commissioner for Human Rights presented her report on the right to privacy in the digital age to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session. In September 2014, a panel event on the right to privacy in the digital age in the context of domestic and extraterritorial surveillance and the interception of digital communications and collection of personal data, including on a mass scale, was convened at the request of the Human Rights Council.[1] Since then, the General Assembly and the Human Rights Council have adopted a number of resolutions reaffirming the importance of the right to privacy and addressing concerns related to arbitrary or unlawful interferences therein.

5. The Human Rights Committee also has raised specific concerns related to the impact of national laws and practices on the right to privacy in its Concluding Observations on the periodic reports of States parties. Concerns also have been raised by Member States through the Universal Periodic Review, with an increasing number of recommendations relating to the right to privacy in the digital space. Special Rapporteur mandate holders also have analysed a range of issues relating to the right to privacy, with specific recommendations to States and other actors.

6. However, many threats to the rights to privacy are yet to be adequately addressed by States. Domestic oversight mechanisms, where they exist, often are ineffective as they fail to ensure transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data. In many States, individuals whose right to privacy may have been violated have inadequate access to an effective remedy. In some countries, there have been attempts to weaken safeguards, such as encryption and anonymity tools that can help to ensure individuals' ability to communicate securely. There is also growing recognition of the role business enterprises play, both in facilitating government surveillance and in their own use of personal information. Businesses often rely on the collection, processing, repurposing and sale of personal information, without ensuring adequate transparency and the informed consent of the individuals concerned.

[1] OHCHR prepared a summary report of the panel (A/HRC/28/39).

III. EXPERT WORKSHOP

Date and Venue

7. The workshop will take place on 19 and 20 February 2018 in Geneva (Palais Wilson, Ground Floor Conference Room). It will start at 10am on 19 February 2018 and ends on 20 February at 1pm.

Participants

8. The expert workshop will bring together States, relevant United Nations bodies, funds and programmes, intergovernmental organizations, treaty bodies, special procedures, regional human rights mechanisms, civil society organizations, academia, national human rights institutions and other relevant stakeholders. Participation of practitioners with specific experience related to the right to privacy and data protection will be encouraged in order to ensure the most practical, detailed and productive discussions.

Methodology

9. The expert workshop will be held in all six official languages of the United Nations.

10. The workshop will seek to encourage the exchange of international, regional and national experiences and practices concerning the protection and promotion of the right to privacy in the digital age.

11. Experts will introduce the themes of the different sessions and interact with participants in order to guide the moderated discussions. Participants, including experts and practitioners from States and other relevant stakeholders, will be invited to share their views, experiences and good practices.

12. Following an opening session, the workshop will be structured around the following main thematic sessions:

Day 1:

Session 1: Setting the scene: role of the right to privacy within the human rights framework and for civic space protection

13. The first session will be dedicated to an overview of the international legal framework governing issues related to the right to privacy, in particular as provided at Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, as the foundation of the right to privacy in human rights law. Other relevant instruments including the UN Guiding Principles on Business and Human Rights and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data will also be discussed. In particular, this session will focus on the importance of the right to privacy as a gateway to the

exercise of other rights by all individuals, including the right to freedom of opinion and expression. In this context, this first session will provide an opportunity to discuss how interferences with the right to privacy can have a chilling effect on civic space and may affect the work of human rights defenders, the media, artists and activists, thereby inhibiting the functioning of a vibrant civil society.

Session 2: Surveillance and communications interception

14. The second panel will examine principles and standards applicable to government surveillance and interception of communications, including the principles of non-arbitrariness, lawfulness, legality, necessity and proportionality, transparency, accountability and non-discrimination. It will cover both the bulk collection, retention and use of personal data and the targeted intrusion into information and communications technology (ICT) systems used by individuals for gathering personal information. Moreover, it will discuss the role of business enterprises in contributing to or facilitating government surveillance activities.

Session 3: Securing and protecting online confidentiality

15. The third session will investigate issues surrounding online confidentiality. It will discuss encryption and anonymity as necessary enablers for the exercise of many human rights, including the right to freedom of opinion and expression. It will also analyse legal and other restrictions on encryption and anonymity imposed by States. Furthermore, panellists will address business enterprises as the main providers of secure information and communications tools and their role vis-à-vis States seeking to weaken the security of information and communications technology in order to obtain personal information. Finally, it will examine ways of protecting the right to privacy by integrating privacy considerations into the design of goods and services (Privacy by Design).

Session 4: Processing of personal data by individuals, Governments, business enterprises and private organisations

16. The last session of the first day will be dedicated to other forms of processing personal data by individuals, Governments, business enterprises and private organisations. One part of the session will examine the increasing reliance of Governments on biometric data, including for mandatory identity cards, the monitoring of public spaces in combination with automated identification, and as a form of identification for obtaining vital services. The session will then turn to corporate practices of data processing and identify human rights-respecting bases for the processing of personal data as well as pertinent data protection principles, such as data minimisation, purpose limitation, data security, data accuracy, and data relevance. Particular attention will be given to the sale, resale and other forms of corporate data sharing and the concentration of immense

amounts of personal data in the hands of corporate actors for purposes such as advertising, credit scoring, and insurance risk scoring.

Day 2:

Session 5: New and emerging issues

17. The second day will start with a discussion of a range of new and emerging issues relating to the right to privacy. The discussion will address various questions that arise with a growing reliance on data-driven technology in an increasingly interconnected world. It will examine how established data protection principles may be operational in this context. The speakers will address in particular the need of anonymization of data to protect the right to privacy of millions of individuals and the issue of the possibility of de-identification of such data through increasingly powerful methods. Finally, the panellists will discuss whether and how groups that may be the target of privacy interferences may enjoy better protection of their rights.

Session 6: Procedural and institutional safeguards, oversight and remedies

18. The last session will turn to practical safeguards against infringements of the right to privacy and remedial avenues for victims. It will discuss different models for ensuring effective, independent oversight, such as a requirement of prior authorisation by an independent body for lawful surveillance and interception, including the request of personal data from business enterprises. Specific concerns related to the importance of effective oversight of intelligence services also will be examined. The session will also discuss remedies that are, or should be available to individuals exposed to unlawful or arbitrary surveillance or interception. Finally, remedial avenues in the context of corporate data processing will also be analysed.

IV. OUTCOME

19. OHCHR will prepare and publish a report on the right to privacy in the digital age, taking into account the discussions at the workshop, as requested by the Human Rights Council in its resolution 34/7. The report will be submitted to the Council at its thirty-ninth session.

Background documents:

- Human Rights Council resolution 34/7, "The Right to Privacy in the Digital Age" of 23 March 2017
- Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37, "The Right to Privacy in the Digital Age"

- Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/28/39, “Summary of the Human Rights Council panel discussion on the right to privacy in the digital age”

- Reports of the Special Rapporteur on the right to privacy, Joe Cannataci, A/71/368, A/72/43103, A/HRC/31/64, A/HRC/34/60

- Reports of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye A/71/373, A/HRC/29/32, A/HRC/32/38, A/HRC/35/22