A message from the United Nations Special Rapporteur on the right to privacy, Prof. Joseph A. Cannataci:

"This is the basic text that will be discussed during the joint public event being held in Rome 18-19 January 2018 and Malta 12-14 February 2018. Further consultation sessions may be announced in the future.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date.

The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion."

Date: January 10, 2018

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

MAPPING WP4

Draft Legal Instrument on Government-led Surveillance and Privacy

Including the Explanatory Memorandum

Ver 0.6

I. Introduction

a. Background

This draft text for a Legal Instrument (LI) on Government-led Surveillance and Privacy is the result of meetings and exchanges between the MAPPING project[1] and several categories of stakeholders shaping the development and use of digital technologies (DTs). These include leading global technology companies, experts with experience of working within civil society, law enforcement, intelligence services, academics and other members of the multi-stakeholder community shaping the Internet and the transition to the Digital Age.

The provisions have been developed using the results of multiple research projects (including MAPPING, RESPECT and SMART).[2] Additionally, international and national best-practices have been taken in account. These insights were combined with the experiences and expertise of all parties involved in contributing to drafting the text which was facilitated by members of the Security, Technology & e-Privacy Research Group (STeP) at the University of Groningen in the Netherlands.

The provisions of the LI are based on international human rights law. Ultimately, this instrument should aid states and the multi-stakeholder community shaping the Internet to protect, respect and promote human dignity. The LI aims at giving clear and detailed guidance for the area of government-led or organized surveillance using electronic means. This is not only necessary for human rights, but also for those who are committed to a responsible and dignified conduct of state authority and powers. The text responds to the challenges arising in the context of law enforcement and intelligence gathering and processing in the digital age.

In the view of the drafters of this document human dignity should be protected, respected and promoted with a holistic approach. Human Rights ought to be considered as one entity, which include the rights of people to develop their lives and personalities in the same way as the rights of victims of crime and of individuals to live in a safe and secure environment.

During the first meetings it transpired that there was a desire to prepare the basis for a new legal instrument covering several problematic issues in the area of government-led or organized surveillance which could form the basis of a new global consensus between states on the matter. Hence, the LI was drafted as a blueprint for any form of soft law or hard law, anything ranging from a non-binding recommendation to a convention or international treaty, which would allow states to join

[1] The MAPPING acronym stands for “Managing Alternatives for Privacy, Property and Internet Governance”. This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345. More information can be found via https://mappingtheinternet.eu/ - accessed on 22.09.2016.

[2] The RESPECT acronym stands for “Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies”. This project has received funding from the European Union’s Seventh Framework Programme. More information can be found via http://www.rug.nl/rechten/organization/vakgroepen/eer/step-research-group/respect_description - accessed on 22.09.2014; The SMART acronym stands for “Scalable Measures for Automated Recognition Technologies”, http://smartsurveillance.eu/ accessed on 13.06.2017.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

the consensus and form a new group which puts emphasis on the promotion and protection of human rights in the Digital Age.

While the infringement of privacy and other rights relating to the development of personality (e.g. freedom of expression) are not new concerns, the violation of these rights in the context of growing use of digital technologies is new, global, complex and constantly evolving. For this reason, States shall provide for shared learning, public policy engagement and other multi-stakeholder collaboration to advance the promotion and protection of these principles and the enjoyment of these rights. Privacy and other rights related to the development of personality shall only be limited when necessary and in a proportionate manner.

However, such measures and general guidance are not sufficient. It is the position of the parties who collaborated on drafting this legal instrument that the protection of human rights by states in the Digital Age must also be outlined in a more detailed and comprehensive way. One of the means for such protection of human rights is through a comprehensive and innovative LI on governmental surveillance, which would assist in establishing safeguards without borders and effective legal remedies across borders.[3]

This instrument applies to all Law Enforcement Agencies (LEA) and Security & Intelligence Services (SIS). While LEA and SIS are organized differently from state to state and the tasks and operational requirements as well as their capabilities differ, the impact of their activities on human dignity and fundamental rights are often similar in nature. Nevertheless, LEAs and SIS have separate functions and - in most States - there is no bulk interception carried out by police.

However, the digital technologies used to carry out surveillance become increasingly similar. Sometimes they are provided by third-party vendors and used by multiple agencies of a state which will be either part of the LEA or the SIS community. The drafters of the LI aimed at developing provisions that fully protect, respect and promote human rights including not only privacy and personality rights, but also public safety, the right to a fair trial and the rights of victims. The impact of surveillance activities on the dignity of humans, regardless of their race, colour, gender, language, religion, political or other opinion, national or social origin, citizenship, property, birth or other status (including age) is at the core of the LI.

To ensure its flexibility when integrated in a specific institutional framework the draft LI is focusing mainly on substantive provisions. Hence, essential procedural provisions relating to a broader legal framework of potentially supranational/national/multilateral nature need to be added if the LI is to become more than a role model or "international gold-standard". This instrument can also be understood to complement the Council of Europe's Cybercrime convention[4] and vice-versa.

b. Methodology

After the introduction and presentation of methodology in Section I., Section II. of this document is divided in two parts.

The following pages include the different sections of the LI, with the text written in *Italic*. Underneath each section follows the text of the proposed explanatory memorandum relevant for that section. The

[3] Cf. First Report of the UN SRP to the Human Rights Council, A/HRC/31/64 via http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc - accessed on 22.09.2016, p.4.
[4] Council of Europe, Convention on Cybercrime, Treaty No. 185 via https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 - accessed on 22.09.2016.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

explanatory memorandum was authored in order to provide context and hopefully facilitate the understanding of the intent of the authors of the draft legal instrument.

Section III. contains the main sources of the document.

This draft has been developed with a strong focus on substance and irrespective of any particular institutional or legislative framework. Hence, many procedural provisions (such as the ones referring to signature and entry into force) are not included.

Furthermore, this draft can also be understood as a proposal to have different agreements which are built on the same foundation and with the same principles in mind. All of the layers are compatible with each other and allow therefore for “upgrading”.

There are three layers:

The basic layer (red) of this text consists of the Preamble, Art. 1, 2, 3, 4, 15, 16 and 17.

The second (yellow) – additional layer of this text consists of layer 1 including Art. 5, 6, 7, 8, 9 and 10.

The third layer (green) consists of layer 1 and 2 including 11, 12, 13 and 14.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

II. Text, Context and Commentary

Preamble

(1) Human rights and fundamental freedoms that people enjoy offline, as enshrined in the Universal Declaration of Human Rights and relevant international human rights treaties, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights, must equally be guaranteed and protected online.

(2) The exercise of human rights on the Internet, in particular the right to privacy and freedom of expression, is an issue of increasing interest and importance as the rapid pace of technological development allows individuals all over the world to use digital technologies (DTs). The access to and use of these technologies is crucial to enable development, especially the development of personality in the digital age. Children, minors and persons developing a gender identity benefit to a very high degree from these new capabilities and opportunities. However, these groups are particularly dependent on efficient safeguards and effective remedies.

(3) DTs can be an important tool for fostering individual and civil society participation. They can be useful in bridging many forms of the digital divide. They contribute to the development of knowledge societies, to the empowerment of women and assist persons with disabilities in participating more comprehensively in public, social, economic and private life. While DTs enable an unprecedented flow of information and create tremendous potential for social and economic development, they also pose new risks and demand concrete actions to transform the essence of human rights to the digital age.

(4) All human rights are rooted in human dignity. Human dignity must be protected, respected and promoted using a holistic approach. Human Rights ought to be considered as one entity, which include the rights of people to develop their lives and personalities as much as the rights of victims of crime and of individuals to live in a safe and secure environment, as well as the right to a fair trial. Each of these rights shall only be limited if necessary and in a proportionate manner while restrictions imposed on rights shall not impair the essence of the right. The impact of the legal framework on the enjoyment of any of these rights should be assessed in its entirety and not limited to specific laws and/or regulations.

(5) It has become increasingly important to build confidence and trust in the Internet, not least with regard to freedom of expression, privacy and other human rights so that the potential of the Internet as, inter alia, an enabler for development and innovation can be realized, with full cooperation between governments, international organisations, civil society, the private sector, the technical community and academia. These stakeholders as well as persons have a responsibility to respect and protect freedom of expression and the right to privacy within their means, particularly in cases where they are controllers and/or processors of personal data.

(6) While concerns about public security may justify the gathering and protection of certain sensitive information, States must ensure full compliance with their obligations under international human rights law. Unlawful or arbitrary surveillance including interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and to freedom of expression and contradict a democratic society founded on the rule of law and human rights.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

(7) Many international and regional systems of law explicitly lay down that in order to restrict/limit/interfere with an individual's enjoyment of the right to privacy a measure, which shall be subjected to independent prior authorization and targeted by nature, must [a] be provided for by a law, [b] pursue a legitimate aim, [c] be necessary and proportionate to the pursued aim [d] while providing appropriate safeguards specified within the law. Furthermore, surveillance activities should be authorized by an independent judiciary or authority whose activities are governed by the rule of law [e] and overseen by a legitimate body [f].

(8) Recognizing that privacy online is essential for the realization of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association, the States which sign this legal instrument declare the following:

The preamble mainly refers to wording that was developed by the United Nations (UN) following the resolution on the Right to Privacy in the Digital Age which also established the mandate of the SRP.[5] It particularly reflects language which can be found in a resolution of the Human Rights Council of 27th of June 2016 on the promotion, protection, and enjoyment of human rights on the internet.[6]

Paragraph (par.) 4 contains a commitment to a holistic approach to human rights which are rooted in human dignity. Ultimately, the entirety of human rights should result in the protection, respect and promotion of human dignity. This is important when considering privacy and other human rights relating to personal development, the right to live in security and the rights of victims of a crime.

Furthermore, this is also important when considering the overall impact of laws relating to governmental surveillance in one country, one region or globally. Such laws and provisions ought to be considered in their entirety and not one by one. The rights concerned in a specific case or situation (apart from absolute human rights like the prohibition of torture or ius cogens rules of international law like the prohibition of genocide) must be considered together and ultimately a solution sought which respects, protects and promotes all human rights – security and privacy, freedom of expression and privacy, etc. LEA and SIS must have the capacity, with appropriate safeguards and oversight, to develop appropriate surveillance to ensure public safety and preserve the right to life and security.

Hence, the focus on freedom of expression and privacy is deliberate, since it allows any (inter)governmental organization to relate to the right to privacy as construed and constructed in the respective binding legal framework. This also allows the text to be flexible.

While all stakeholders have a responsibility to respect and protect fundamental rights also in a digital context it remains clear that this can only happen within their means. Among the stakeholders mentioned, states clearly have the responsibility of controlling law enforcement requests and national security agencies practices. States should not only refrain from infringing these rights on a domestic and international level, they should also protect and promote them domestically and internationally and support an environment which enables their citizens to develop their personalities freely and positively.

[5] United Nations, Human Rights Council Resolution 28/16. For more sources see the sources provided at the end of this document.

[6] United Nations, Human Rights Council, A/HRC/32/L.20.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

The term "measure" in par. 7 relates to an act by a state or on its behalf or at its order which as an effect derogates from the right to privacy of an individual.

Par. 7 also adds the requirement in lit. c for any limitation of a right to be necessary and proportionate. Here, as everywhere in this text those terms should be understood in the following way: Necessity is referring to the specific end or purpose ("telos") of a measure. Necessity should be prescribed by law which itself must be the result of a legitimate legislative process. Typically, necessity is a purpose that is legitimate in a society which is based on values such as human rights, rule of law and democracy.

If a measure is necessary, a proportionality assessment shall be carried out following a three-step test: First, the measure which is taken must be potentially capable of realizing the aim. Secondly, the measure which is taken is required to reach the aim (in other words it must be the least-intrusive measure). Thirdly, the measure which is taken must be proportionate "strictu sensu". This means that it is not only a capable measure which is the least intrusive one (steps 1 and 2), but also legitimate considering its impact on the overall situation and particularly other human rights potentially infringed during the process. Only if all these three criteria are met, is a necessary measure also proportionate.

To learn further about regional examples mentioned in par.7 one can consult the case of the European Court of Human Rights (ECtHR) in the case of Zakharov vs. Russia.[7] Particularly, the notions of the abstract nature of surveillance (mn. 171) and the requirement of the foreseeability of surveillance (mn. 229) have been discussed.[8] Another regional example to be considered is the judgment of the Court of Justice of the European Union (CJEU) in the joined cases C-203/15 and C-698/15 Tele 2 Sverige and Watson.[9] The targeting of a surveillance measure has been discussed in mn. 109 - 111. Necessity is discussed in mn. 118 – 121.

Further cases that should be considered from the Inter-American System of Human Rights are Donoso v. Panama and Escher et al. v. Brazil.[10]

Article 1

Subject matter and objectives

(1) The subject matter of this legal instrument is electronic surveillance. It aims at safeguarding the fundamental rights and freedoms of individuals with regard to the deployment and use of surveillance systems, as well as non-surveillance data when used for surveillance purposes. These surveillance measures will duly take into consideration security concerns and corresponding operational needs with a view to meet the obligations of states to ensure the security of the individuals they are responsible for.

[7] ECtHR, Roman Zakharov v. Russia, App. No. 47143/06 via http://hudoc.echr.coe.int/eng?i=001-159324 accessed on 28 February 2017; General principles are being discussed in mn. 227 -234.
[8] Ibidem.
[9] CJEU, Tele 2 Sverige, C-203/15, ECLI:EU:C:2016:970,
[10] Inter-American Court of Human Rights, Case of Tristán Donoso v. Panamá, Judgment of 27.01.2009 also available via http://www.corteidh.or.cr/docs/casos/articulos/seriec_193_ing.pdf - accessed 25.10. 2017; Ibid., Case of Escheret al. v. Brazil, Judgment of 20.11.2009 also available via http://www.corteidh.or.cr/docs/casos/articulos/seriec_208_ing.pdf - accessed 25.10.2017.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

(2) In accordance with this legal instrument, States shall ensure the implementation of the measures herein to protect the fundamental rights and freedoms of individuals when a surveillance system is used, as well as when non-surveillance data are used for surveillance purposes.

(3) Surveillance systems as well as the use of non-surveillance data should be designed and function to ensure the right to privacy, notably through the use of privacy-enhancing technologies and in accordance with the achieved state of technological knowledge and operational capabilities.

The formulation "legal instrument" is an interim one and is capable of being substituted by the term "Recommendation" or "Directive" or "Treaty" or "Convention" depending on the binding force that parties may wish to accord the instrument. It is intended that this draft legal instrument is capable of being used in part or in whole by regional intergovernmental organisations such as the European Union (EU) or the Council of Europe (CoE) or indeed even at the global level by the UN. This is consistent with the MAPPING project's finding that, when it came to surveillance everywhere and particularly on the Internet, there was no discernible difference between the concerns of stakeholders inside Europe and of those outside Europe. The concerns were as universal as the right to privacy set out in Art 12 UDHR/Art 17 ICCPR, Art 8 of the European Convention on Human Rights and Art 7/8 of the EU Charter of Fundamental Rights as well as similar provisions laid down in equally relevant regional protection mechanisms such as Art 11 of the American Convention on Human Rights.

It may also be used by States wishing to have a set of principles on which to model their domestic law until a regional or global agreement is reached and to which they could conceivably adhere.

Article (Art.) 1 defines the subject matter of this legal instrument. It addresses surveillance carried out by using or manipulating electronic devices. Such activities are carried out by States on their behalf or on their order. While most of these activities will be carried out online using the Internet, it is also possible that other electronic technologies are being used. The legal instrument is not aiming at covering conventional surveillance in the physical world, but surveillance using or facilitated by digital technologies and typically over the Internet.

However, not only direct efforts of States to gather information electronically are covered. Information received from other States or data repurposed from parties in other countries beyond their jurisdiction are subject to this text, too.

This legal instrument refers to governmental surveillance and tries to provide an answer to the issues raised in instances such as the revelations of Edward Snowden, the blocking of Internet services by governments with little or no justifiable arguments, and the questions that arise while studying cases such as Apple vs the FBI.[11] The formulation *"with a view to meet the obligations of States"* in the last sentence of par. 1 emphasizes this perspective.

Furthermore, the legal instrument is drafted to tackle these challenges from a perspective which has international human rights protection and human dignity at its centre.

Par. 1 is concerning the right of all persons in the jurisdiction of a State, not only citizens.

[11] More information on this and encryption is in the First report of the SRP to the UN General Assembly, available via http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx - accessed on 22.09.2016.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

Par. 2 should not be read as balancing security against privacy or any other fundamental human right. In the view of the drafters it is necessary that fundamental human rights are promoted in a comprehensive manner. Rather than a trade-off between rights, ways should be sought to strengthen them collectively and to ultimately promote human dignity. Hence, it is necessary to provide both privacy and security rather than the one or the other.

Par. 3 refers to the basic setup of technologies of surveillance which should follow an approach where the purpose and aim of the activities are clearly laid out before information is gathered. Information gathering should be strictly limited to what is necessary and proportionate.

Article 2

Definitions

For the purpose of this legal instrument, the following definitions shall apply:

(1) 'surveillance' is any monitoring, collecting, observing or listening by a state or on its behalf or at its order to persons, their movements, their conversations or their other activities or communications including metadata and/or the recording of the monitoring, observation and listening activities.

(2) 'surveillance system' refers to any organised means or resources designed, and/or intended to be used for surveillance.

(3) 'smart system' refers to a system which incorporates functions of sensing, autonomous decision-making and actuation.

(4) 'smart surveillance system' means a smart system used for surveillance.

(5) 'surveillance data' is data the primary purpose for the creation of which is surveillance and/or non-surveillance data actually being used for surveillance. This includes data the primary purpose for the creation of which is surveillance and gathered as a result of acts by a State or on its behalf or at its order without the use of a dedicated surveillance system.

(6) 'non-surveillance data' is data the primary purpose for the creation [or collection] of which is not surveillance, but which [could be] [is?] searched or interrogated because the data contained therein may, through either pattern recognition or applied search methods yield personal data which may be useful for the prevention, detection, investigation and prosecution of crime and/or for increasing public-safety, and/or protecting state security.

(7) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(8) 'controller' means the competent public authority, agency or other body or natural or legal person which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by domestic law, the controller or the specific criteria for its nomination may be provided for by domestic law.

(9) 'competent authority' means any public authority competent for the prevention of a real danger and/or the prevention, detection, investigation and prosecution of crime and/or for

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

increasing public safety and/or protecting state security; or any other body or entity entrusted by State law to exercise public authority and public powers for these purposes.

(10)'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

(11)'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, [creation], recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, destruction, or the carrying out of logical and/or arithmetical operations on such data.

This Art. provides the definitions needed to understand the text of the legal instrument.

Par. 1 defines surveillance as an act of government or entities which act on behalf of the government. This is reflected in the wording "*by a state or on its behalf or at its order".* The definition is kept broad intentionally to cover all possible aspects of governmental surveillance.

The term "surveillance" includes all forms of bulk acquisition of personal data[12], all forms of mass surveillance and targeted surveillance. This sentence is also intended to cover all those instances where the surveillance activity is carried out by non-state actors acting on behalf of or at the order of any form of state authority.

Surveillance is only acceptable if it is based on reasonable suspicion.[13] However, reasonable suspicion is not a standard that is defined in international law outside Europe. When deciding whether

[12] As adapted from the UK Government's Operational case for bulk powers (2016 – see https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf :

Through the bulk interception of communications . This involves intercepting international communications as they travel across networks.

Through bulk equipment interference. This involves the acquisition of communications and equipment data directly from computer equipment overseas. Historically, this data may have been available during its transmission through bulk interception. The growing use of encryption has made this more difficult and, in some cases, equipment interference may be the only option for obtaining crucial intelligence.

As bulk communications data, obtained from communications service providers. Communications data can be invaluable in identifying the links between subjects of interest and uncovering networks.

As bulk personal datasets. This involves the use of datasets such as travel data or Government databases. Like communications data, the information included in those datasets is generally less intrusive than data acquired through equipment interference or interception.

[13] CJEU, Tele 2 Sverige, C-203/15, ECLI:EU:C:2016:970, mn. 103: "Further, 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 […]."

reasonable suspicion exists, it is necessary to demonstrate that the specific anticipated surveillance will yield evidence of a serious crime or help mitigate the threat.

Most of the time surveillance might be carried out through the collection and processing of data as referred to in par. 6 (*'surveillance data' is data the primary purpose for the creation of which is surveillance and/or non-surveillance data actually being used for surveillance).*

Nevertheless, the legal instrument also refers to data which was originally collected for other purposes and is being re-used for surveillance as defined in par. 6. In such cases data, which was originally non-surveillance data, also becomes surveillance data according to par. 7. The main characteristic to distinguish surveillance and non-surveillance data is the original purpose for the creation of the data.

Both, the definition of surveillance data in par. 6 and non-surveillance data in par. 7 include not only the actual content of conversations, messages, activities etc., but also metadata generated about it.

The definition in par. 8 (personal data), par. 11 (processor) and par. 12 (processing) are the same as in the General Data Protection Regulation of the European Union (GDPR) and its Article 4.[14]

The term *"natural person"* was used therefore in par. 8. It is possible that legal persons (like corporations) are entitled to fundamental rights like privacy or similar rights in different States. However, since the situation differs from State to State and because of different legal traditions in different states it is left to them to decide whether they choose to extend protection to legal persons or not.

The definition in par. 9 (controller) is similar to the one in Art. 4 (7) of the GDPR, but has been modified to be consistent with the rest of the legal instrument.

The definition of par. 10 (competent authority) is based on the definition of Art. 3 (7) of the Directive (EU) 2016/680.[15]

Article 3

Basic requirements for government-led surveillance

(1) No surveillance, domestic or foreign, civil or military, may be carried out except by a law enforcement agency (LEA) or a Security and Intelligence Service (SIS) or any public-mandated entity (PME) tasked by a specific law.

(2) This law shall be publicly available. The provisions shall meet a standard of clarity and precision that is sufficient to ensure that individuals can foresee its application.

(3) Any law regulating surveillance shall aim at the prevention of a real danger and/or the prevention, detection, investigation and prosecution of crime and/or for increasing public safety and/or protecting state security. The surveillance itself must be necessary and proportionate and the least intrusive means shall be used.

(4) LEAs and PMEs shall include tax, revenue, customs and anti-corruption authorities. SIS shall include all forms of intelligence and security services, whether civil, military or signals intelligence, foreign or domestic.

[14] EU, Official Journal L 119/33, 04.05.2016

[15] EU, Official Journal L 119/89, 04.05.2016.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

(5) No surveillance, except that of foreign military personnel, serving members of LEAs, SIS and PMEs may be carried out by any entity the existence of which is secret. All LEA, SIS and other PME authorized by law to conduct surveillance shall be created and governed by laws which shall also provide adequate safeguards against the abuse of powers and particularly surveillance.

(6) These safeguards shall include but shall not be restricted to a system of checks and balances consisting of:

- *a. Legislative oversight on a regular basis and at least quarterly, by a Committee of the regional or national elected legislative body responsible for the entity's funding and tasked for the purpose by law, of the budgetary and operational performance of all LEAs, SIS and PMEs authorized by law to carry out surveillance, both domestic and foreign, with the authority to temporarily or permanently withhold, suspend, grant or cancel the funding of any surveillance programme or activity;*
- *b. A Pre-Authorisation authority, completely independent from the entity and the executive or legislative branches of government, composed of one or more members with the security of tenure of, or equivalent to, that of a permanent judge which is tasked by law to evaluate ex-ante requests from and grant permission to LEAs, SIS and PMEs as shall be required under law prior to the conduct of lawful surveillance;*
- *c. An Operational Oversight authority, completely independent from the entity, the Pre-Authorisation Authority and the executive or legislative branches of government, composed of one or more members with the security of tenure of, or equivalent to, that of a permanent judge which is tasked by law to exercise ex-post oversight over and exercise accountability of LEAs, SIS and PMEs as shall be required under law especially for the conduct of lawful surveillance;*
- *d. Inter-institutional whistle-blower mechanisms that allow for anonymity of the whistle-blower(s) and include extra-authoritarian and/or extra-institutional review of the process including remedies;*
- *e. The presentation and publication of reports, at minimum on an annual basis, by the Legislative, Pre-Authorisation and Operational Oversight Authorities.*

(7) Any LEA, SIS or PME carrying out surveillance must be explicitly authorised to do so and regulated by a specific law defining the

- *a. Purposes.*
- *b. Tasks.*
- *c. Objectives.*
- *d. Activities.*
- *e. Basic administrative functions and setup.*

(8) Any surveillance activity must only be carried out for concretely defined specific and legitimate purposes and in response to a concrete and legitimate need. Except in those cases where it concerns serving foreign military personnel, serving foreign LEA, SIS or PME officers, all surveillance, domestic and foreign, shall be carried out only provided that a relative warrant is obtained ex-ante from the regional or national pre-Authorisation Agency in the case of persons or data located within the regional or national jurisdiction, or that an International Data Access Warrant (IDAW) is obtained from the International Data Access Commission (IDAC) as created in terms of Article 15 of this legal instrument, or provided that a valid legal request is obtained

ex-ante under a legal framework for cross-border requests that includes the relevant regional or national government authorities.

(9) When any form of warrant for surveillance is requested, the only criteria that may be taken into account is that of reasonable suspicion. The race, colour, gender, language, religion, political or other opinion, national or social origin, citizenship, property, birth or other status alone of the suspect cannot be advanced or accepted as being adequate or relevant grounds for the issue of any form of surveillance warrant.

(10)Any law authorising surveillance must include intelligible, accessible and effective procedural remedies for individuals concerned.

(11)The budget of any entity carrying out surveillance must be defined clearly and subject to review on the executive, political and judicial level, albeit when necessary and appropriate the review process may be carried out in camera.

This article defines the basic requirements a government must fulfil when carrying out surveillance (as defined for the purposes of this text).

Par. 1 states that any surveillance activity must be based on a specific law. The term surveillance shall be understood broadly since it includes domestic and foreign oriented activities and includes civil and military actions.

There are overall three types of entities that are potentially able to carry out surveillance: LEAs (typically providing inner security and stability), SIS (typically providing external security and stability) and public mandated entities (PMEs; can be private contractors).

A specific law is also required to regulate activities for PMEs. For example, the ECtHR made clear that the State cannot absolve itself from responsibility by delegating its obligations to private bodies or individuals.[16]

When surveillance is carried out through PMEs the government always remains in full control of, and fully responsible for, the entire surveillance process, data, and use and further processing of data. The outsourcing of surveillance activities to PMEs may divert responsibility away from police, judicial or national security departments and onto small companies that cannot be held accountable to constitutional prohibitions. Therefore, private entities that are involved in the surveillance process must be subject to stringent deontological rules and confidentiality requirements, and be under a contractual obligation to provide full transparency and governmental access to their technical and organisational arrangements governing the surveillance activities. State entities must be provided with sufficient expertise and resources in order to be able to remain in full control of any surveillance activities that are outsourced to private entities.

Furthermore, “LEAs and PMEs shall include tax, revenue, customs and anti-corruption authorities” which suggests a broad understanding which is also applicable to SIS.

The specific law provides increased legitimacy for surveillance activities. It enables a better understanding for the need to carry out surveillance. Additionally, it becomes more likely that the

[16] ECtHR, Wos v Poland, App.No. 22860/02, 01.03.2005.

general scope of activities is subject to a broad discussion while details regarding individual operations must not necessarily be disclosed. Such a law should also be containing which kind of information is being collected and which authorities can access the data under which circumstances. Additionally, it should be laid down how the data is being managed once it has lost relevance.

According to par. 3 the specific law supports States in their efforts to maintain the basic order of a society. The purposes of surveillance are therefore defined as "*prevention of a real danger and/or the prevention, detection, investigation and prosecution of crime and/or for increasing public safety and/or protecting State security.*"

It is not necessary to separately include "the economic interest of the State" since serious crimes relating to it can legitimize surveillance per se. Industrial espionage or other activities that enable the unauthorized use of intellectual property are not legitimate purposes to carry out surveillance.

The terms necessity and proportionality as well as the criteria to establish them have already been discussed and described in the explanatory memorandum of the preamble. See there for more information.

Par. 5 clarifies that there are no secret parts of a State which carry out any kind of surveillance. Those LEAs, SIS or PMEs who carry out surveillance do so in an environment with safeguards including a system of checks and balances.

This system (par. 6) consists of regular and effective legislative oversight (lit. a), an independent pre-authorisation authority (ex-ante oversight, lit. b), an independent operational oversight authority (ex-post oversight including accountability of LEAs, SIS and PMEs, lit. c), inter-institutional whistle-blower mechanisms (lit. d) and the presentation and publication of separate reports compiled by the legislative oversight, independent pre-authorisation and independent operation oversight authority (lit. e). These measures are supposed to reinforce each other and are a complete system. In the understanding of the drafters of this document, oversight is not a finished product. Rather it is constant work in progress.

On the notion of independence in this section and other sections of the text see also the "Basic Principles on the Independence of the Judiciary" and numerous treaty-based standards and comments on this subject that are collected by the Office of the High Commissioner for Human Rights.[17]

Par. 8 forbids any surveillance measures that are being carried out without a concrete purpose and/or objective. It is forbidden to carry out any surveillance for the mere collection of information or potential future use apart from any concrete threat or case. Additionally, such a threat must legitimize the limitation of human rights. Any measure taken must therefore be necessary, governed by law and proportional (suitable to achieve the aim, necessary to achieve the aim – least intrusive method, proportional in the sense that other rights/societal interests do not override).

[17] For an online version of the UN Basic Principles on the Independence of the Judiciary see: http://www.ohchr.org/EN/ProfessionalInterest/Pages/IndependenceJudiciary.aspx - accessed 25.10.2017.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

Except in those cases where it concerns serving foreign military personnel, serving foreign LEA, SIS or PME officers the system if the International Data Access Warrant (IDAW) is being introduced. More on this mechanism can be found in Art. 15.

Par. 9 forbids any surveillance based on discriminatory motives. Any surveillance must be based on reasonable suspicion and leave out any other motives to start an investigation. Reasonable suspicion exists against the target of the surveillance, rather than simply a reasonable suspicion that exists generally. It refers to the "*race, colour, gender, language, religion, political or other opinion, national or social origin, citizenship, property, birth or other status"* of a person. The term political or other opinion also includes philosophical beliefs. The term other status can be read as also referring to age and the rights of children and elderly people. This also applies to other sections of the text where this list of characteristics is used.

Par. 10 establishes remedies for any individual concerned by a surveillance measure. Often it is hard for individuals to establish how their human rights have been affected concretely. Furthermore, the phrasing individuals makes clear that such an individual must not be a citizen of a particular country. While the detailed circumstances of such a (often judicial) review procedure must not necessarily be disclosed any party to this agreement must guarantee that a meaningful review takes place and that individual human rights are being protected, respected and promoted when carrying out surveillance activities.

Par. 11 refers to the budget of entities carrying out surveillance. The budget must not be disclosed in detail necessarily, but it must be subject to checks and balances, external evaluation and review. In many countries this will be done through legislative control such as parliamentary control.

Article 4

General Principles

When considering the use of surveillance systems, as well as the use of non-surveillance data for surveillance purposes, States shall adhere to the following principles:

(1) States shall provide that surveillance systems shall be authorised by law prior to their use. This law shall,

a. identify the purposes and situations where the surveillance system is to be used.

b. define the category of serious crimes and/or threats for which the surveillance system is to be used.

c. state that the agency using the surveillance system should only use the system in cases where a reasonable suspicion exists that a serious crime and/or threat may be committed;

d. define and provide the least intrusive measures which potentially might be suitable to achieving the aim.

e. demand from the authority to justify that each single measure envisaged is strictly necessary and proportionate for the obtaining of vital intelligence in an individual operation as well as considering the overall impact of this and such measures on the

right to privacy of individuals irrespective of whether the individual is a citizen or resident of that State.[18]

f. *provide that any final decision on enacting the surveillance system shall be subjected to independent prior authorization before actual surveillance takes place.*

g. *provide that the deliberate monitoring of an individual's behaviour by the State should only be targeted surveillance carried out on the basis of reasonable suspicion.*

h. *provide that the individual concerned is likely to have committed a serious crime or is likely to be about to commit a serious crime and in all such cases such domestic law shall establish that an independent authority, having all the attributes of permanent independent judicial standing, and operating from outside the law enforcement agency or security or intelligence agency concerned, shall have the competence to authorise targeted surveillance using specified means for a period of time limited to what may be appropriate to the case.*[19]

i. *provide that where the person to be subjected to targeted surveillance and personal data pertaining to that individual are to be found outside the jurisdiction of the state then the law enforcement agency or the security service or intelligence agency concerned would be empowered to apply for an International Data Access Warrant (IDAW) to the International Data Access Authority (IDAA) set up in terms of this legal instrument.*

j. *ensure that all public and private entities within the jurisdiction of the State would comply with the requirements of a properly constituted International Data Access Warrant (IDAW) immediately with the same effect as if that warrant had been issued by a court established within that particular State. In such cases the domestic law should provide that territoriality or jurisdiction cannot be raised as a reason or a defence for the public or private entity concerned not complying with an IDAW request to hand over or otherwise make accessible the personal data requested.*

k. *state that the authority carrying out the surveillance shall, unless an independent authority has adjudicated that it would not be appropriate or feasible to do so and/or this would be prejudicial to the completion of ongoing or future investigations or the prevention, detection or prosecution of a specific criminal offence or threat, without undue delay [within a period of time established by law] explain in writing the use of the surveillance system in the particular situation to any person who was directly or indirectly subject to such surveillance.*

l. *set the length of time information obtained from the surveillance system should be kept and whom it may be accessed by at each stage.*

[18] This provision can be understood in connection with the ECtHR judgment in Szabo and Vissy v Hungary, App. No. 37138/14, para. 73. The second part is inspired by the German constitutional court's development of a holistic approach (Überwachungsgesamtrechnung) to the extent of surveillance in society declaring that a measure of precautionary surveillance cannot be examined in isolation, but must always be seen in the context of the totality of the existing collections of data on the citizens as established in BVerfG, 1 BvR 256/08 [2010], paragraph 218

[19] ECtHR, App. No. 47143/06, Zakharov vs. Russia, via http://hudoc.echr.coe.int/eng?i=001-159324 – accessed on 22.09.2016. Mn. 264: "[…] it must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such information may be made by names, addresses, telephone numbers or other relevant information."

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

m. set up an independent surveillance oversight authority to monitor the conduct of surveillance and ensure that the provisions of the law are followed.

n. provide for an individual right to redress for subjects of surveillance.

(2) States should set up and promote procedures to ensure transparency about and accountability for government demands for surveillance data and non-surveillance data for surveillance purposes. Such procedures should include, but are not limited to:

a. Publicly available, periodic reports allowing for a substantive and comprehensive review of the activities of relevant agencies to other State entities such as the legislative branch and/or the judicial branch of a State.

b. Publicly available transparency reports by the State itself in respect to all requests made to corporations and other non-state actors with regard to the provision of personal data including categories, and frequency.

c. Provide for transparency regarding surveillance law regulations and the power of agencies who carry out surveillance.

d. Setting up of a documented, regular and ongoing process of dialogue with civil society and academia and other stakeholders on the purpose and design of surveillance systems and the use of non-surveillance data for surveillance purposes.

e. Support and encouragement of publicly available transparency reports by corporations and other non-State entities which provide personal data if the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale. States must not prohibit corporations from publishing transparency reports.

(3) When considering the use of surveillance systems, as well as the use of non-surveillance data for surveillance purposes, States should respect and protect the free flow of information and the stability of information and communication technologies and services. Particularly, States are prohibited from directly or indirectly ordering or compelling

a. service providers in their jurisdiction to disconnect, shut down access or otherwise broadly disrupt or block flows of information. If in an individual case a State agency has reasonable suspicion that a particular service was set up and/or is being used substantively for an illegal purpose a service provider may be required to deny that service on the presentation of a legal request issued pursuant to applicable laws in accordance with the rule of law. Any such limitation must be necessary and proportionate as well as limited to the extent of such illegal use.

b. service and hardware providers to take measures which negatively impact the security – particularly the security of technologies such as encryption – of digital services or products.

c. that actions are taken which require data localization.

d. that agencies carrying out an investigation and seek to use information held by private entities deceive their intentions.

e. a lowering of standards through legislative or other measures of the protection of privileged communications and records of privileged communications.

(4) When setting up and operating surveillance systems, as well as while using non-surveillance data for surveillance purposes, States shall

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

a. not assert extra-territorially jurisdiction over data or persons in contravention of relevant treaties and principles of international mutual legal assistance.

b. seek to establish appropriate bilateral and/or multilateral international legal frameworks to facilitate cross-border requests for data in a manner that adheres to the rule of law and is consistent with international human rights principles.

(5) If States share intelligence

a. such activities shall be subject to an oversight regime equivalent to and as effective as described in Art. 3 par. 6.

b. they are required to ensure that oversight authorities have access to any relevant information necessary to evaluate the legality, necessity and proportionality of the sharing and the agreements that form the basis of such activities.

c. they shall empower oversight authorities to review decisions and/or undertake independent investigations concerning the activities.

d. they shall ensure that this information is only shared with states that have equivalent, effective and adequate mechanisms in place to guarantee similar standards and safeguards.

This Art. defines the General principles states should be adhering to when carrying out surveillance activities.

The phrase in par. 1 "*authorised by law*" should be interpreted with reference to the categories laid down in European Court of Human Rights (ECtHR) judgment in the case of Roman Zakharov vs. Russia.[20] Particularly, authorised by law means that there is an actual request for surveillance, a certain level of suspicion (e.g. reasonable suspicion as interpreted in this document later on), impartial and effective oversight of the activities, authorization by judicial warrants and no bulk collection of information. The latter principle of no bulk collection has since been very strongly entrenched in European law by the decision of the European Court of Justice in Sverige2 and Watson of 21 December 2016.[21]

Furthermore, States must identify the purposes and situations where the surveillance system may be used to a degree of granularity beyond the general purposes of national security or crime prevention.

Par. 1 was created to contain a proportionality assessment, but reaches further than that. It additionally contains provisions on how to handle a case where surveillance was used after the information was gathered.

Targeted surveillance is only acceptable if is based on reasonable suspicion as mentioned in par.1 lit. c.[22] However, reasonable suspicion is not a standard that is sufficiently defined in international law

[20] ECtHR, App. No. 47143/06, Zakharov vs. Russia, via http://hudoc.echr.coe.int/eng?i=001-159324 – accessed on 22.09.2016. Mn. 260 defines that an independent authority charged with authorising surveillance "must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security."

[21] CJEU, Tele 2 Sverige, C-203/15, ECLI:EU:C:2016:970.

[22] CJEU, Tele 2 Sverige, C-203/15, ECLI:EU:C:2016:970, mn. 103: „Further, 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,

except possibly outside European Law. When deciding about whether reasonable suspicion exists, it is necessary to demonstrate that the specific anticipated surveillance will yield evidence of a crime or help mitigate the threat. This also applies to the level of suspicion that must exist to act in accordance with par. 4 lit. a.

The requirement in par. 1 lit. d that the surveillance system defines the least intrusive measures has to be interpreted as being the "least intrusive means for achieving the legitimate aim in the particular circumstances." To make sure this is the case other less invasive techniques should have been considered or it must be obvious from the outset that they are futile.

In par. 1 lit. k a time limit is mentioned. Here, as well as in the rest of this legal instrument, time limits are set in square brackets as an indication of urgency of a procedure. However, each time limit may have to be amended to address the special circumstance and criminal procedural law in the respective State. The time limits need to fit the operational and managerial practices of a State. Nevertheless, time in most of the procedures covered by this legal instrument is of the essence. Large delays in action may result to delays in justice and hence reduced effectiveness of safeguards ("Justice delayed is justice denied.")

Par. 2 makes it mandatory for states to be transparent about the surveillance systems they employ. They should also be required to explain how they are using them in principle. In this way, an ordinary citizen should be able to understand the potential scope of surveillance activities. This is very important, because in the absence of such an understanding it is not possible for citizens in a democratic society, to legitimize the activities of LEAs and SIS.

Par. 2 lit. a and b oblige States to setup a transparency report system both internally ("checks and balances") as well as externally for the public record. When doing so - as mentioned in 4.2.7. of the Council of Europe Recommendation on Internet Freedom - oversight bodies involved in the process should be empowered to obtain access to all relevant information held by public authorities, including information provided by foreign bodies.[23] Furthermore, States should periodically evaluate their implementation of human rights standards, including with respect to surveillance activities.

This should be augmented through broader exchanges with civil society and relevant stakeholders (lit. c).

According to lit.e States must support/encourage private entities to report on the requests made to them. This applies to all relevant private entities as long as the "*core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.*" This exemption typically removes this obligation for small and medium sized corporations or other small-scale private entities as long as these do not carry out activities which are of particular interest to the state and the public in the context of passing on private data to public entities for the purpose of surveillance.

---

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 […]."

[23] Council of Europe, Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom, via https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2016-5-of-the-committee-of-ministers-to-member-states-on-internet-freedom?_101_INSTANCE_aDXmrol0vvsU_viewMode=view/ accessed 31.07.2017.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

Par. 3 is an obligation for States to create an environment which promotes the development of the potential of DT regardless of territorial or protectionist considerations.

Par. 3 lit. a refers to shutting off the access to information networks broadly and indiscriminately. The formulation also refers to a situation where the network is slowed down on purpose and becomes practically useless. The phrase "limited to the extent of such illegal use" can refer to the suspension of a specific user account or similar measures.

If State authorities reasonably believe that a particular service or site was setup for illegitimate purposes or is being used substantively for an illegal purpose then it might be justified to shut down that specific service. However, this must only be done *to the extent of such illegal use and* upon the *"presentation of a legal request"* or in other words in the context of a fair procedure which is governed by the principle of the rule of law, subject to independent and impartial oversight and respecting the "equality of judicial arms" principle.

Par. 3 lit. b refers to the need to guarantee the security of information products and services. States are banned from trying to weaken the development of security standards by requiring developers and/or engineers to intentionally weaken the implementation of protective technologies. This specifically prohibits states from banning any forms of encryption, requiring a service provider to maintain keys or the ability to decrypt data, and requiring a service provider to weaken encryption. It also prohibits states from requiring that a service provider create so-called "backdoors" and/or any other technological measures designed to circumvent security measures that are intended to protect the users of the service.Par. 3 lit. c focuses on the issue of data localization and retention. States should be obliged to refrain from ordering other entities to locate or store data.

Par. 3 lit. d makes it mandatory for State authorities to make their intentions clear when they interact with corporations and other private entities. This serves to reinforce the principles by which the purpose and aim of an operation should be clearly set out before personal data is gathered.

Par 3 lit. e obliges States to not lower the standards of protection of *"privileged communications"*. States should not pressure journalists or members of the press to disclose sources or limit the freedom of press in an unjustified manner. States should establish specific legal procedures to safeguard the professional privilege of groups such as members of parliament, members of the judiciary, lawyers and media professionals. More on the nature and circumstances of privileged communications can be found in the explanatory memorandum to Art. 5 par. 1 lit. a vii.

Par. 4 makes it clear that States should not try to impose territorial restrictions through regulatory measures when technologies are cross-border in nature. States should not try to get access to data not stored on their territory by putting corporations or citizens under pressure because they or their offices are physically located on their territory. In general, States should aim at establishing an international framework of cooperation in those cases where law enforcement or information gathering is needed in a cross-border scenario. This framework should be based on human rights principles and should allow for technology to develop its full potential.

Par. 5 addresses the issue of intelligence sharing between countries. At the time of drafting this legal instrument this seemed to be an increasingly relevant activity to protect public order and safety and to protect the rights of victims of crime. Hence, it should be ensured that the same standards and principles are relevant for cross-border surveillance as for national surveillance activities.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

The term "intelligence sharing" refers to (1) sharing of "processed" intelligence, (2) sharing of "raw" personal and/or meta-data, (3) direct access to data, (4) joint operations of states to collect intelligence.

Article 5

Domestic Measures related to the deployment of surveillance systems

(1) States shall provide that no new surveillance system can be deployed:

a. before an initial human rights impact assessment is carried out by an independent external assessment body with the objective of ensuring that privacy and other human rights are protected in accordance with the provisions of this instrument. The human rights impact assessment must include analysis of:

i. proportionality and necessity of the surveillance system;

ii. technological security and state of art of the technology used;

iii. actions taken to minimise the risks to the enjoyment of rights of individuals;

iv. compliance with privacy by design and privacy by default principles;

v. safeguards to ensure that personal data collected during surveillance is not kept when no longer necessary for the purposes for which it was collected;

vi. social and ethical costs of deploying the surveillance system. Such costs must be given due consideration and mitigation measures have to be sought where appropriate;

vii. safeguards in place to protect privileged communications.

b. before the report of the initial human rights impact assessment in par. 1 was submitted to the applicable competent authority, which can ask for additional measures to be introduced before the deployment of the surveillance system can start.

c. unless an initial testing of the surveillance system, carried out by an independent external assessment body, shows that adequate security means have been put into place to prevent illegal access to the personal data, and to the algorithms of the smart surveillance system by unauthorised persons or systems.

d. in the case of smart surveillance systems, the error rate is below the threshold established for similar systems by a technical advisory body set up for this purpose or submitted for human assessment in terms of Article 9.

(2) For existing surveillance systems, a human rights impact assessment which fulfils and is equivalent to the requirements for new surveillance systems as laid down in par. 1 of this provision has to be finalized no later than 12 months after the ratification of this agreement by a state party.

(3) Any surveillance measure using systems that comply with this article is subject to a judicial warrant.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

This article refers to states and the measures they need to take if they want to carry out surveillance activities.

Par. 1 lays down the detailed criteria of a "human rights impact assessment" which is mandatory before the deployment of surveillance systems. Par. 2 mirrors the same criteria for existing surveillance systems.

Par. 1 lit. a refers to an "*independent external assessment body"*. Such a body should consist of formally independent experts from different parts of the domestic stakeholder community (civil society, government, corporations, data protection authorities, etc.) who have access to all information necessary to evaluate the deployment of a concrete surveillance system. These experts also have to have the necessary qualification and assistance (resources) to effectively evaluate the system and report to the authority responsible for the deployment of the system. The competent authority responsible for the deployment of the system itself has to subject to political and/or judicial oversight (checks and balances).

Par. 1 lit. a iii could include measures relating to the use and development of data mining algorithms. Such activities should be subject to regular assessments of the likely impact of the data processing on the rights and fundamental freedoms of data subjects. The basic structure of the analysis should be based on predefined risk indicators which have been clearly identified in advance. The relevance of individual results of such automatic assessments should be carefully examined on a case-by-case basis, by a person in a non-automated manner.[24]

Par. 1 lit. a vii refers to *"privileged communications"*. There is a variety of such relations that various legal systems may recognize (e.g. spousal relations, caregiver or guardian relations, parent-child relations, parliamentary privilege, clerical relations, journalist-source, etc.). This also includes specifically protected professions and the privileged communications they might have with patients or clients (such as doctors or lawyers). The protections are to be defined in detail by a member states domestic law. Only communications falling outside the scope of the privilege may be intercepted.

Par. 1 lit. d sets up a similar requirement to that established in Par. 1 lit. a, but for smart surveillance systems. A "*technical advisory body"* should have the same basic qualities as an independent external assessment body. More emphasis has to be set however, on the qualification of members since smart surveillance systems typically require more specific, technical and contextual knowledge than is needed for the evaluation of the deployment of surveillance systems in general.

Article 6

Domestic Measures related to the use of surveillance systems

(1) States shall provide that the use of surveillance systems will not continue:

a. before a human rights impact assessment is carried out by an independent external assessment body with the objective of ensuring that privacy and other human rights are protected in accordance with the provisions of this instrument. The human rights impact assessment body must be satisfied that, inter alia,

[24] Council of Europe, T-PD(2016)18rev, 19.08.2016.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

i. The use of the surveillance system is necessary and proportionate;

ii. effective actions have been taken to minimise the risks on the enjoyment of rights of individuals while operating the surveillance system;

iii. the surveillance system is designed and operated to comply with privacy by design and privacy by default principles; ;

iv. processes that reflect the operational needs are in place to inform the data subject that his/her personal data is being kept;

v. personal data collected during surveillance is not kept when no longer necessary for the purposes for which it was collected, nor is it kept for longer than the time allowed for by law;

vi. personal data kept is accurate and current;

vii. use of the personal data follows the purposes permitted by law;

viii. the sharing of the personal data with other authorities is carried out only as permitted by law, limited to what is necessary and proportionate and in compliance with international human rights law;

ix. systems of redress for data subjects are in place;

x. safeguards which protect privileged communications are in place;

xi. adequate security means have been put in place to prevent illegal access to the personal data, and to the algorithms of a smart surveillance system by unauthorised persons or systems;

xii. social and ethical costs of deploying the surveillance system have been considered. Such costs must have been given due consideration and mitigation measures be sought where appropriate.

b. unless the report of the annual human rights impact assessment is to be submitted to the applicable competent authority, which can require additional measures to be introduced for the continuation of the deployment and use of the surveillance system.

(2) In the case of smart surveillance systems, States shall provide that the use of surveillance systems will not continue unless annual testing of the system shows that the error rate is below the threshold established for similar systems by a technical advisory body set up for this purpose or submitted for human assessment in terms of Article 9.

The "*independent external assessment body"* mentioned in Par. 1 lit. a should have the same qualities as mentioned in the commentary on Art. 5. States are free to choose whether this can be the same body or not. However, members of the body must have formal independence and the substantial knowledge required to carry out the assessment as well as the resources required to do so effectively.

Par. 1 lit. a x. refers to *"privileged communications"*. Such communications are to be defined by a member states domestic law and have already been described in the explanatory memorandum to Art. 5 par. 1 lit. a vii. These laws typically include lawyers, doctors and other professions which rely on confidentiality between a client and the protected professional. Only communications falling outside the privilege may be intercepted.

The "*technical advisory body"* mentioned in Par. 2 is similar as described in the commentary on Art. 5. States are free to choose whether this can be the same body or not. However, members of the body

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

must have formal independence and the substantial knowledge (particular emphasis on this criteria) required to carry out the assessment as well as the resources required to do so effectively.

Article 7

Domestic Measures related to the use of non-surveillance data

(1) States shall provide legislation identifying the conditions for the use of non-surveillance data for the purposes of surveillance. This law should, inter alia, as appropriate:

a. identify the purposes and situations where non-surveillance data are to be used.

b. ensure that the data was originally produced for purposes compatible with the purposes.

c. define the category of serious crimes and/or threats for which the non-surveillance data are to be used.

d. ensure that the agency using the non-surveillance data should use data in cases where reasonable suspicion exists that a serious crime may be committed or that a serious threat may exist.

e. ensure that the agency carrying out the surveillance shall, unless it would not be appropriate or feasible to do so and/or this would be prejudicial to the completion of ongoing or future investigations or the prevention, detection or prosecution of a specific criminal offence or adequate mitigation of threat, without undue delay [within a period of time established by law] explain in writing the use of the non-surveillance data in the particular situation to the person who was directly or indirectly subject to such surveillance.

f. set the length of time information obtained from non-surveillance data should be kept.

g. set up an independent and adequately resourced oversight body to monitor that the provisions of the law are followed.

(2) States shall provide that access by law enforcement agencies and security and intelligence services to and use of non-surveillance data may not continue for surveillance purposes unless an annual human rights impact assessment, including an assessment on proportionality and necessity of the access and use of non-surveillance data is carried out by an independent external assessment body and the assessment body is satisfied that, inter alia,

a. the risks on the enjoyment of rights of individuals are in place regulating the way non-surveillance data is accessed and used.

b. privacy enhancing technologies are being used and documented.

c. processes that reflect the operational needs, are in place to inform the data subject that his/her personal data is being processed and stored.

d. non-surveillance data is not kept when no longer necessary for the purposes for which it was collected or for the time allowed by law.

e. personal data kept is accurate and current.

f. use of the non-surveillance data follows the purposes permitted by law.

g. only proportional and necessary sharing of non-surveillance data with other agencies is taking place or could take place and in all such cases only as provided for by law.

h. systems of redress for data subjects are in place.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

i. adequate security means have been put in place to prevent illegal or unauthorized access to the non-surveillance data.

j. social and ethical costs of using the non-surveillance data are being given due consideration and mitigation measures sought.

(3) The report of the annual human rights impact assessment of par. 2 is to be submitted to the applicable competent authority, which can ask for additional measures to be introduced for the continuation of the deployment and use of non-surveillance data.

(4) States shall provide that access or use of non-surveillance data must not have the effect of singling out individuals on the basis of race, colour, gender, language, religion, political or other opinion, national or social origin, citizenship, property, birth or other status, data concerning health or data concerning a natural person's sexual activity or gender the controller shall implement effective protection to minimize impact and introduce adequate safeguards in accordance with the achieved state of technological knowledge as well as additionally requiring, where appropriate, judicial authorisation.

This Art. clarifies that there must be a specific law in place in a State that allows for the request of such information from private entities. States should provide adequate resources to ensure that LEA and SIS are educated and remain informed about the current state of technology and potential impacts on human rights.

Allowing authorities to always ask for information should not become a standard routine. While, LEAs and SIS are, potentially, interested in proving that they have not missed out on anything in the course of an investigation, the request for information should always be based on a standard consistent with international laws and norms (including international human rights laws and norms -e.g., reasonable suspicion).

Targeted surveillance is only acceptable if is based on reasonable suspicion.[25] However, reasonable suspicion is not a standard that is sufficiently defined in international law. When deciding about whether reasonable suspicion exists, it is necessary to demonstrate that the specific anticipated surveillance will yield evidence of a crime or help mitigate the threat against public safety.

The "*independent external assessment body"* mentioned in par. 2 should have the same basic qualities as mentioned in the commentary on Art. 5. States are free to choose whether this can be the same body or not. However, members of the body must have formal independence and the substantial knowledge required to carry out the assessment as well as the resources required to do so effectively.

Article 8

Right to notification

[25] CJEU, Tele 2 Sverige, C-203/15, ECLI:EU:C:2016:970, mn. 103: „Further, 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 […]."

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

(1) States shall provide that where a surveillance system or non-surveillance data is used for surveillance purposes, the individual subject of the surveillance (whether directly or incidentally) has a right to notification.

(2) States shall provide that the authority carrying out the surveillance shall, unless an independent authority has adjudicated that such notification constitutes an abuse of this provision or that this would be prejudicial to the completion of ongoing or future investigations or the prevention, detection or prosecution of a specific criminal offence or threat, without undue delay [a period between four hours and seven days] explain in writing to the individual subject of the surveillance, the use of the surveillance system in the particular situation.

(3) States shall provide that the explanation should

a. contain in clear and plain language meaningful information about the logic used in the (smart) surveillance system;

b. contain the reasons for which the individual has been subject to surveillance;

c. mention the existence of the right to request from the data controller the rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;

d. mention the right to lodge a request for human assessment referred to in Article 8 and the details of the office responsible for processing the request.

(4) States shall provide appropriate safeguards where the person subjected to surveillance is a minor. These safeguards may include that the parents or guardians of the minor are to be informed on behalf of the minor and may exercise any rights in his/her name.

(5) Where, pursuant to par. 2, a State does not notify an individual, it must ensure that there is a redress procedure in place to enable individuals to contest surveillance without having to first establish that they had been subject to a surveillance measure.

(6) If states have decided that monitoring by private entities falls under the definition on surveillance for the purposes of this legal instrument, potential subjects of surveillance have the right

a. to be informed when entering an area which is being monitored. A notification or sign must contain clear and meaningful information about the logic used in the (smart) surveillance system;

b. to know the reasons upon which the individual is subject to surveillance;

c. to be informed about the right to lodge a request for human assessment referred to in Article 9 as well as about the details of the office responsible for processing the request.

This article provides an individual right that any subject of surveillance is entitled to know that it has been the target of governmental surveillance. It supports 'a right to know' of the individual unless an independent authority (e.g., an independent judicial authority) has adjudicated pursuant to the rule of law that disclosure would prejudice the operation of law enforcement. In some cases there may be an issue with notifying individuals that they are under surveillance as this may lead to compromising an investigation. A delay in disclosure may be needed to protect officers from harm or may be needed to enable LEAs and/or SIS to establish the identities of other perpetrators.

The wording *"specific"* points to the fact that the potential harm must be tangible or relating to an actual and known event which is likely to occur. Potential dangers, which cannot be linked to an existing set of facts, are not sufficient to justify the delay of the notification.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

As is outlined in par. 2 such a notification shall be phrased in a clear language, detailed (par. 3) and delivered close to the actual event.

In par. 2 the phrase "*that such notification constitutes an abuse of this provision"* refers to potential cases where such notifications will be abused to intentionally overburden the system or where individuals intentionally abuse this right to gain a better understanding of the strategic setup of state authorities carrying out surveillance without being predominantly interested in a specific case which is the cause for surveillance. However, it is crucial that such a decision is taken by an independent authority which is not directly responsible for issuing the notification. Additionally, some countries issue notifications to people who are not named in the order legitimizing surveillance, but if it is in the interests of justice. This is a good practice for States to follow.

Par. 4 relates to the surveillance of minors who also have a right to be informed. This right, however might be exercised through their parents or guardians.

Par. 5 relates to monitoring carried out according to Art. 2 par. 2. Individuals who enter an area where they are likely to be subject of monitoring should be informed of that fact. They should be made aware of the surveillance system being employed (e.g. camera system). The information might also be backed up with symbols (camera icons or images, etc.). Usually, this will be done by installing signs in the area where surveillance is carried out. If smart technology is used to interpret the pictures this should also be indicated.

Additionally, individuals should be provided with reasons for having been subjected to surveillance. Typically, these reasons should be based on the domestic law. However, it is also useful to give additional explanations in plain language.

Any operational activity, specifically when smart surveillance systems are employed, is subject to a human assessment process as lined out in Art. 9.

Article 9

Right to Human assessment

(1) States shall provide that an individual who alleges that the use of a surveillance system or non-surveillance data for surveillance purposes has led to, inter alia, unjustified:

- *a. restrictions imposed while entering the territory of a State;*
- *b. restrictions on right of free movement and/or right to assembly and association;*
- *c. limitations or restrictions on other fundamental rights or freedoms;*
- *d. detention and/or arrest;*
- *e. placing on black lists/watch lists;*
- *f. awarding of fines or penalties;*

has the right to request a human assessment by an officer appointed for this purpose.

(2) States shall provide that the aim of the human assessment is to carry out an objective examination, by a person not initially involved in the surveillance or the effects of the surveillance, of the facts used in the decision-making process. States shall provide

- *a. how the process of human assessment will take place;*

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

b. how the rights of the individual to be informed; to be heard; to remain silent; to engage legal counsel as well as other basic procedural rights will be protected;
c. the legal effects of the outcome of the human assessment;
d. the right to lodge a complaint to the Appeals Board referred to in Article 10;
e. that a human assessment will be conducted without being prejudicial to the completion of an ongoing investigation or future investigation or the prevention, detection or prosecution of a specific criminal offence or threat.

(3) The officer appointed for this purpose shall initiate the process of human assessment without undue delay [a period between four hours and seven days] from when such a request is made.

(4) The officer appointed for carrying out the human assessment shall within a reasonable period [between four hours and seven days] examine the use of the surveillance systems and shall, unless an independent authority has adjudicated that a written explanation of the outcome of the human assessment would be prejudicial to the completion of an ongoing investigation or the prevention, detection or prosecution of a specific criminal offence or threat, without undue delay explain in writing the outcome of the human assessment carried out.

(5) In cases where the officer comes to a beneficial conclusion for the individual concerned immediately, States restore the original condition effectively and promptly.

(6) In cases where a decision is taken in accordance with par. 5 and restoration to original condition is impossible, States shall provide for adequate, prompt and effective compensation for the infringements suffered.

A Human assessment is not a Human Rights Impact assessment. The more there are automated means of assessment, the more there is a need for the possibility of a human actually analysing the decision. Officers appointed for this purpose must be trained to understand the system and not to rely too much on its judgement. All of this must be ensured as part of the compliance process with this system. This human assessment may, in the jurisdictions where this is applicable, be likened to 'merits review procedures'.

The list in par. 1 has to be understood as being descriptive. It is possible that States decide to add a Human Rights Assessment for similar procedures.

Par. 3 identifies the process which can be set in place for these safeguards to have effect. This par. also gives a suggestion of the time period within which the procedure should take place.

Another time limit is mentioned in Par. 4. When deciding on the actual time limit it may be pertinent to consider practical considerations such as language needs. In border control cases, for example, the individuals concerned may require translation or other types of language services as they do not speak the language of the country on whose border they are.

Par. 5 demands a possibility to give the officer making a decision also the competence to restore the original and justified state ("restitutio in integrum") with little administrative effort. Hence, an individual concerned will have a quick and effective remedy.

Par. 6 obliges states to compensate in cases where the restoration of the original condition is impossible.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

Article 10

Right to appeal

(1) States shall provide that the human assessment taken by the officer and the facts giving rise to the human assessment can be subject to appeal to an Appeals Board specifically set up to review the effects of the surveillance system or non-surveillance data. The Appeals Board is to call a hearing without undue delay [a period between four hours and seven days] from the moment the individual submits his/her request.

(2) States shall provide that as far as practicable, the Appeals Board will give its decision without undue delay [a period between seven days and three months] from the moment when the request was submitted.

(3) States shall provide that the burden of proof lies on the controller of the personal data, who must prove that the surveillance system or non-surveillance data was used in accordance with laws, regulations, rules or procedures in force and in line with fundamental rights protection.

(4) States shall provide that where the controller cannot without undue delay [a period between eight hours and one month] prove that the surveillance system or non-surveillance data was used in accordance with laws, regulations, rules and procedures in force and in line with fundamental rights protection, then the appeals board shall order:

a. the reversal of the effects, as far as practicable.

b. compensations for any damages, including moral damages, suffered by the data subject.

c. the data held about the data subject upon whom the effect of the surveillance system was based to be rectified or deleted. The data controller responsible for carrying out the rectification or deletion is to carry out the decision forthwith and inform the individual in writing on the action that was taken.

d. if appropriate, the review of the deployment of a surveillance system or the non-surveillance data practices.

(5) States shall provide that within 24 hours from the lodging of an appeal, the competent authority which has the authority over the processing of personal data by the controller shall be notified of the on-going appeal. The competent authority has the right to intervene in the proceedings.

(6) States shall provide that appeals against the decision of the Appeals Board can be made to the competent court.

(7) In cases where restoration to original condition is impossible, States shall provide for adequate, prompt and effective compensation for the infringements suffered.

If the subject of surveillance is not satisfied with the outcome of the Human assessment an appeal might be made to an *"Appeals Board specifically set up to review the effects of the surveillance system or non-surveillance data".* The appeal can be made regardless of the original result. However, the findings of the appeals board must not lead to a decision which is worse for the individual concerned than the one taken by the officer who did the human assessment (no "reformatio in peius").

Given that different jurisdictions have different Appeals Boards/Courts, it is up to each State to set up an Appeals Board in line with the legal culture and preferences in that State. However, the appeals

board must be capable and resourced in a way that allows a fair trial.[26] The members of such a board must have the necessary training to understand the technological background of the surveillance system and the impact the produced data might have on the subjects of surveillance.

This board will most likely be a quasi-judicial body consisting of experts (selected on criteria of qualification and seniority) on the surveillance system which is subject to review. The appeals board should consist of members from the state (LEAs and/or SIS community) and data protection specialists (academia and/or data protection officers).

The size of the board and its composition depend on the surveillance technology that is being overseen. While the members of the board have to be free and independent in their individual decision making, they do not have to fulfil the same criteria of institutional independence as judges. However, the decisions of an appeals board must be based upon the existing legal framework which needs to be in accordance with international human rights standards, including the holding of fair hearings as part of the appeal process.

The decision of the Appeals Board can be appealed against to the competent court.

Compensation provided following par. 4 lit. b shall be adequate, prompt and effective. Restoration to original condition should be sought where possible.

Article 11

Surveillance system security

(1) States shall provide that adequate safeguards are put in place to protect the data processed by a surveillance system against risks violating its integrity, confidentiality, availability and resilience.

(2) States shall provide that the controller shall be responsible for establishing an information security management system based on internationally accepted standards and based on a risk assessment conducted for the establishment of the information security management system for this purpose.

(3) States shall provide that the controller shall be responsible for developing the communication infrastructure and databases in order to preserve the security of data, in compliance with a security policy established for this purpose.

(4) States shall provide that the controller is responsible for defining authorization or security-clearance procedures for its staff for each level of data confidentiality.

(5) States shall provide that the controller is responsible for notifying the relevant competent authority, without undue delay, when a data breach of a surveillance system has taken place. This notification must be provided in a manner not prejudicial to the completion of an ongoing investigation or the prevention, detection or prosecution of a specific criminal offence or threat.

This article relates to the technical aspects of system security for surveillance systems. States shall ensure that the systems are secure and in compliance with *"internationally accepted standards"* (par.

[26] For guidance on the notion of a fair trial see Council of Europe, Guide on Article 6 of the ECtHR via http://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf - accessed on 13.03.2017.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

2) which also includes that they are in accordance with the achieved state of technological knowledge, in other words that they are state of the art. For example, relevant ISO standards might be used for guidance.[27]

The security aspect does not include hardware and software considerations, but refers mainly to the challenges of proper management of these systems. Hence, there is a need for education and training of the staff involved in their operation (par. 4).

Article 12

Supervision of users of surveillance systems

(1) States shall provide that controllers regularly ensure that their users observe all the relevant legal rules related to the use of surveillance systems including those assuring the quality, accuracy and time limitation placed upon data.

(2) States shall provide that the relevant competent authority has the power to supervise the activities of controllers of surveillance systems and can carry out spot checks and checks of processing incidents.

(3) States shall provide that the controller shall take all necessary measures to correct or to ensure the correction of possible processing errors.

(4) States shall provide that any abuse of a surveillance system by the user should be considered as an aggravated offence.

This provision relates to the administrative supervision of surveillance systems. Authorities and entities involved in surveillance must make sure that there are internal procedures in place which ensure compliance with substantive legal provisions.

In relation to par. 1 it must be assured that data is only accessed for a limited amount of time and only as long as necessary and proportionate to comply with the goal of this Art.

States shall develop additional training standards in compliance with international reference frameworks. Limited access to data could be assured according to the Standard ISO/IEC 29115:2013, which provides a framework for managing entity authentication assurance in a given context.

Article 13

Monitoring the use of surveillance systems

(1) States shall provide that the relevant competent authority may request from the controller any information on the use of each individual surveillance system being deployed by the controller.

(2) States shall provide that a controller subject to such monitoring must provide the requested data.

[27] More information on the International Organization for Standardization (ISO) is at https://www.iso.org/standards.html - accessed 27.10.2017.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

States should not only setup an internal compliance procedure but also ensure that there are checks and balances across the institutions of the State. Hence, the relevant competent authority has the obligation to setup a procedure which reviews the activities of SIS and LEAs.

Article 14

Multi-Stakeholder Approach, and Collaboration

(1) States shall provide for shared learning, public policy engagement and other multi-stakeholder collaboration to advance the promotion and protection of fundamental rights and freedoms in the digital age in connection with surveillance.

(2) In order to facilitate this process States shall support permanent fora for international dialogue to maintain and develop common standards, practices and technological safeguards relating to the protection of fundamental rights and fundamental freedoms in the digital age in connection with surveillance. This shall also include fora for exchange between state authorities carrying out surveillance and all stakeholder groups who shape the development of DTs.

By signing up to this legal instrument States express their commitment to support Human Rights in the Digital Age. This means that they will not only refrain from certain behaviour, but that they will actively contribute to creating an environment which is beneficial for the development of individuality and personality through modern DTs. As a precondition for this, fundamental rights such as privacy and freedom of expression must not only be protected and respected, but also promoted.

This can only be achieved by commitment to a regular and ongoing exchange with all members of the multi-stakeholder community who shapes events in the digital age.

States are free to choose whether they will set up new or adapt existing fora to achieve these aims collectively. They may choose to do so as parties to this agreement or in other appropriate contexts.

States are furthermore encouraged to consider involving members of oversight bodies created by this legal instrument in the multi-stakeholder exchange fora.

Article 15

Mechanisms for transborder access to personal data

(1) States shall establish an International Data Access Authority with the purpose of protecting personal data, privacy, freedom of expression and other fundamental human rights while facilitating the timely exchange of personal data across borders as may be required for the legitimate purposes of law enforcement agencies, intelligence and security services.

(2) The International Data Access Authority (IDAA) shall be comprised of:

a. The Surveillance Legal Instrument Consultative Committee (SCC),

i. comprising of one member nominated by each contracting party;

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

ii. which shall meet at least twice a year at the Headquarters of the International Data Access Authority;

iii. monitor the workings of this legal instrument;

iv. make recommendations as to the acceptance of new parties to the legal instrument;

v. make recommendations on the interpretation and eventual amendment of the legal instrument.

b. The International Data Access Commission (IDAC),

i. comprising of a number of independent judges nominated by each of the contracting parties;

ii. shall decide upon all requests for the granting of an International Data Access Warrant (IDAW) which may be submitted by law enforcement agencies, security or intelligence services of a contracting State;

iii. When carrying out the function of par. 2 lit. b ii the IDAC shall decide in the following way,

1. each request for an IDAW shall be heard by a panel of three judges each from separate jurisdictions one of whom should be a judge in the jurisdiction from where the request originated;

2. Except for the judge from the jurisdiction originating a request, all judges on a panel will be assigned to adjudicate each request for an IDAW at the initial request stage, through automated random allocation;

3. The Chair of the Panel should always be a judge from a jurisdiction other than that from the one where the request for the IDAW originated from;

4. Where the request impacts more than three jurisdictions or where, in the opinion of the Panel Chair, the complexity of the case so merits, the Panel shall, at the request of the Panel Chair, be composed of five Judges each from different jurisdictions;

5. All decisions of the Panel shall be taken by simple majority. Dissenting opinions may be recorded at the express wish of the dissenting Judge or Judges.

c. The International Committee of Human Rights Defenders (ICHRD),

i. compromising of eminent independent human rights experts, one from each contracting party or more pro rata if the workload so requires;

ii. whose member experts (HRD) shall be nominated by contracting States and be able to demonstrate excellent knowledge in the fields of human rights including privacy, freedom of expression and freedom of association;

iii. whose member experts (HRD) shall be assigned to monitor the proceedings followed by the International Data Access Commission and the International Data Access Tribunal where such proceedings are carried out in camera;

iv. shall, once a year, after internal meetings and deliberations, present to the Consultative Committee a report on the number of cases monitored, the difficulties encountered in such cases and include in such annual report recommendations on bad practices to be avoided and best practices to be

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

followed in the protection of human rights and the authorisation and carrying out of surveillance;

v. A Human Rights Defender (HRD) will be assigned to monitor each request for an IDAW at the initial request stage,

1. the selection of the HRD shall be based on automated random allocation;

2. A HRD shall have the right of audience and to present arguments on behalf of but unknown to the data subject concerned, where it is felt that such surveillance requested is unnecessary, disproportionate or in any way breaches that individual's fundamental human rights.

d. The International Data Access Tribunal (IDAT),

i. comprising of a number of judges nominated by each of the contracting parties;

ii. which shall decide upon any and all appeals resulting from the refusal of the International Data Access Commission to grant an IDAW;

iii. an appeal may be submitted in exceptional circumstances, such as the availability of new evidence by law enforcement agencies, security or intelligence services of a contracting State;

iv. each appeal shall be heard by a panel of five judges each from separate jurisdictions one of whom should be a judge in the jurisdiction from where the request originated;

v. except for the judge from the jurisdiction originating a request, all judges on a panel of the IDAT will be assigned to adjudicate each request for an IDAW at the initial appeal stage, through automated random allocation;

vi. the Chair of the Panel should always be a judge from a jurisdiction other than that from the one where the request for the IDAW originated from;

vii. where the request impacts more than three jurisdictions or where, in the opinion of the Panel Chair, the complexity of the case so merits, the Panel shall, at the request of the Panel Chair, be composed of seven Judges each from different jurisdictions;

viii. all decisions of the Panel shall be taken by simple majority. Dissenting opinions may be recorded at the express wish of the dissenting Judge or Judges.

e. The International Data Access Authority Administration (IDAAA) which shall provide all the administrative, logistical and other support services required for the Authority to carry out its functions in a timely and efficient manner.

(3) The International Data Access Authority (IDAA) shall model itself on best practices especially those utilised to deliver cost-effective dispute resolution in an on-line environment:

a. Any and all proceedings of the IDAA may and should wherever possible and appropriate be carried out on-line.

b. proceedings carried out in person at the Headquarters of the IDAA will only be permissible in those exceptional instances where the Panel Chair obtains the explicit written permission from the Chair of the Surveillance Legal Instrument Consultative Committee.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

c. Secure video-conferencing and other communications facilities shall be provided by the IDAAA in order to enable the judges and Human Rights Defenders to carry out their duties.

(4) The contracting parties to this legal instrument shall provide the adequate resources for the efficient working of the IDAA;

a. Human Rights Defenders and Judges nominated by States shall, for the period of their service to the IDAA, be remunerated directly by the Authority under such terms and conditions to be established by the Consultative Committee.

b. The financial contribution of each contracting State shall be determined by the Consultative Committee in accordance with the GDP, size of population and number of requests for IDAW originating from or directed to a particular State.

(5) Any contracting State which does not make its financial contribution, or nominate its Judges, or Human Rights Defenders in a timely manner shall be automatically suspended from the membership and benefits of the this legal framework for a period of two years from the due date of payment of contribution or nomination.

(6) Any contracting State which carries out surveillance upon the activities of or otherwise attempts to interfere with the workings of the IDAA is automatically suspended from the membership and benefits of the this legal framework for a period of five years from the discovery of such surveillance or interference.

(7) Any State applying to become a party to this legal framework which carries out surveillance upon the activities of or otherwise attempts to interfere with the workings of the IDAA is hereby automatically determined to be ineligible for the membership and benefits of the legal framework for a period of five years from the discovery of such surveillance or interference.

States and other stakeholders should work together to develop legal frameworks that (a) provide for governments' cross-border requests for user data between or among relevant regional or national governments, (b) respect the sovereignty and jurisdiction of each State, (c) adhere to the rule of law, and (d) protect human rights and public safety. Proposals for such legal frameworks have included bi-lateral and multilateral agreements. This provision outlines, for further multi-stakeholder discussions, one approach for such a legal framework.

This Art. creates the cost-effective, privacy-friendly mechanisms which would enable States to request and receive access to personal data held in other States, but which could be important to the detection, investigation and prosecution of serious crimes including terrorism and organised crime. The creation of the International Data Access Authority (IDAA) created by this Art. would facilitate cross-border investigation and surveillance through the International Data Access Warrant (IDAW) contemplated earlier in Art. 5. This would be complementary to mechanisms existing within States to grant authorisation for surveillance and would kick in at the request of the law enforcement agency or the security or intelligence service of a contracting party once it was clear that there is – as is now very often the case – a transborder, multiple jurisdiction dimension to the location where personal data may be held. The mechanism created by this legal instrument could notionally create a privacy-friendly one-stop shop for LEAs and SIS to apply for the IDAW which could greatly reduce costs and delays in data transfers at both the domestic and international levels. The request would be speedily dealt with by a panel of 3-5 judges in an on-line manner similar to the way that on-line dispute resolution operates successfully today in various other domains including WIPO and TLD issues. Each request would be

monitored and assured by an independent human rights defender, this measure partially inspired by the innovative practice introduced by the USA's FISA court.

In a world where personal data is increasingly held by private companies in data centres which are established in accordance with rules dictated by technical and financial expediency, it would also become much simpler for a company to handle a request for personal data coming from a law enforcement or national security or intelligence agency located outside a particular jurisdiction: if the company is presented with an IDAW it can rest assured that such a warrant was issued in full protection of human rights and authorised by the law of the State where its data centres are located – which would presumably be a party to this legal instrument.

The creation of such a mechanism would, if the IDAA is properly resourced and staffed, cut down waiting times for transfer of personal data required by law enforcement, prosecutors and intelligence services by weeks and often by an average of up to eleven months. With panels of judges working world-wide in a secure on-line manner, on a rota 24/7, urgent requests for access to personal data, whether in real-time or historical, for legitimate surveillance purposes could be handled quickly and efficiently.

Article 16

Application to public and private entities

(1) The controller and the processor shall be bound by the provisions of this instrument if the processing is carried out by a competent authority, any other public authority or body, or on behalf of or at the order of any of these public entities.

(2) States may determine that monitoring by private entities using electronic means falls under the definition of surveillance in Art. 2 par. 1, if such monitoring is in place for the purposes the prevention of a real danger and/or the prevention, detection, investigation and prosecution of crime and/or for increasing public safety and/or protecting State security.

(3) In cases where a State decides to expand this legal instrument to monitoring by private entities in alignment with the definition Art. 16 par. 2, such entities shall be bound if the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.

(4) If a State decides to make use of the option in Art. 16 par. 2 of this legal instrument, it shall notify the other parties of this legal instrument after signing and before domestic ratification of this legal instrument takes place.

This clause emphasizes the focus of the provisions of this legal instrument which is surveillance carried out through or on behalf of the government.

Par. 2 provides an addition that States can opt-for when joining this agreement. It refers to monitoring by private entities that States might choose to regulate as 'surveillance'. This includes but is not limited to Closed Circuit Television (CCTV), any class of sensors/actuators that are not smart (e.g. gunshot

detector or the sound of glass cracking/breaking, etc.) as well as the collection of information emanating from portable telephones, or internet use.

Such monitoring must only be included if the intent to carry it out is surveillance for *"the prevention of a real danger and/or the prevention, detection, investigation and prosecution of crime and/or for increasing public safety and/or protecting State security.*" Hence, such surveillance must have the same purpose as the surveillance activities described in par. 1. Additionally, it must be carried out on a scale that is meaningful to contribute to the four aims mentioned in par. 1 and par. 2.

As an example, the contributors to this document have discussed the cooperation among private operators of CCTVs in shopping malls and their cooperation with law enforcement, in cases where the decision on how to de-escalate critical situations rests with the private operators. (In case of an incident they could ask themselves: "Should we call the police or leave the issue for the local security service or some special social workers who know the perpetrators better?" The choice of the action which is leading to resolving the situation quickly and most efficiently is left to the private entity carrying out the monitoring.).

However, since the situation in certain States is different, parties to the legal instrument may choose on their behalf whether or not to extend the provisions of the legal instrument to these technologies and scenarios.

However, as pointed out in par. 3, this is not true in all cases. That is why this legal instrument covers only private entities *"if the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale."*

For example, a small shop which uses 5 cameras to avoid shoplifting would not fall under this definition, while a large regional shopping mall or department store with a large number of cameras would.

Par. 3 sets a timeframe for States on when to communicate their intention to apply this legal instrument, including to private CCTV operators.

Article 17

Extended protection

(1) None of the provisions of this legal instrument shall be interpreted as limiting or otherwise affecting the possibility for a State to grant data subjects a wider measure of protection than that stipulated in this text.

(2) None of the protections identified in this document are designed to limit or derogate from the rights provided by the United Nations Universal Declaration of Human Rights (particularly Art. 12) and the United Nations International Convention on Civil and Political Rights (particularly Art. 17) or other international treaties a State has ratified that improve the level of protection of a data subject within the scope of this instrument.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

This provision is a standard clause in Human Rights Law treaties and inspired by the wording of Article 11 in the modernized version of Convention 108 of the Council of Europe.[28] It defines that the provisions in the legal instrument have to be understood as setting a minimum level and that States are free to improve standards of protection if they wish.

The international agreements referred to in par. 2 are the Universal Declaration of Human Rights by the United Nations as proclaimed in Paris on 10 December 1948 (General Assembly resolution 217 A) and the United Nations International Covenant on Civil and Political Rights Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976. Other noteworthy international agreements and guidelines are for example, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) by the Council of Europe as well as the Convention on Cybercrime of the Council of Europe (CETS No.185), the revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) of the Organisation for Economic Cooperation and Development and Privacy Framework of the Asia-Pacific Economic Cooperation.

[28] Cf. Consolidated version of the modernised convention 108 (September 2016) via https://rm.coe.int/16806a616c – accessed on 28.07.2017, p. 5.

This text attempts to reflect and put up for discussion the many views received by the Special Rapporteur to date. The Special Rapporteur does not necessarily agree with all parts of the text which are included, but is presenting them in the spirit of open discussion. An annotated version containing all comments received in an anonymized form will be made available separately in order to further facilitate further in-depth discussion.

III. Sources

- UN Legal Framework (particularly Art 12 and Art 19 of the Universal Declaration of Human Rights and Art 17 and Art 19 of the International Covenant on Civil and Political Rights).
- Several UN resolutions (particularly resolution 68/167 of 18th of December 2013 on the right to privacy in the digital age as well as 28/16 of 24th of March 2015; a resolution of the Human Rights Council of 27th of June 2016 on the promotion, protection, and enjoyment of human rights on the internet, A/HRC/32/L.20; Resolution A/HRC/34/L.7/Rev.1 on the right to privacy in the digital age of 22nd March 2017).
- Principles from https://www.reformgovernmentsurveillance.com/ - accessed 13.12.2017.
- GNI Principles: https://globalnetworkinitiative.org/principles/index.php - accessed 13.12.2017.
- International Principles on the Application of Human Rights to Communications Surveillance from https://necessaryandproportionate.org/principles - accessed 13.12.2017..
- Recommendation CM/Rec(2010)13 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00 – accessed 13.12.2017.
- Modernization process of Convention 108 of the Council of Europe; http://www.coe.int/en/web/data-protection/modernisation-convention108 - accessed 13.12.2017.
- Council of Europe, Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom.
- EU Fundamental Rights Agency (FRA) report "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update", via http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega - accessed 13.12.2017.
- Several judgments of courts like the ECtHR, Roman Zakharov v. Russia, App. No. 47143/06; Szabo and Vissy v Hungary, App. No. 37138/14; CJEU, Tele 2 Sverige, C-203/15, ECLI:EU:C:2016:970.
- RESPECT Toolkit.
- Input from participants received in preparation and during the MAPPING meetings in Washington (April 2016), Malta (June 2016 and May 2017), New York (September 2016), Miami (February 2017) and Paris (September 2017).
- Written submissions received from various rounds of consultation with different members of the multi-stakeholder community.