Contribution to Open Consultation on UN GGE 2015 Norm Proposals

Yuval Shany*

1. Introduction

Human Rights Council resolutions 20/8 (2012) and 26/13 (2014) on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167(2013) and 69/166 (2014) on the right to privacy in the digital age, mentioned in the call for open consultation, appear to be premised on a number of general normative propositions:

- That the same rights that people have offline must also be protected online;
- That the nature of the internet is *global*, *open* and *interoperable*;
- That the Internet can be an important tool for development and for exercising human rights;
- That States should facilitate access to the internet, and that and international cooperation should be aimed at the development of media and information and communication facilities and technologies in all countries;
- That States should address on-line security concerns in accordance with their international human rights obligations, including through national democratic, transparent institutions, based on the rule of law;
- That there is a need for human rights to underpin internet governance, and states should, through transparent and inclusive processes with all stakeholders, adopt national Internet-related public policies;
- That governments should engage with all relevant stakeholders, including civil society, private sector, the technical community and academia, in protecting and promoting human rights and fundamental freedoms online;
- That business enterprises have a responsibility to respect human rights as set out in the Guiding Principles on Business and Human Rights.

* Hersch Lauterpacht Chair in Public International Law, Hebrew University of Jerusalem; Senior Fellow, Israel Democracy Institute; Vice-Chair of the UN Human Rights Committee.

The resolutions further underscore that technological development enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights (in particular, the right to privacy); and that freedom of expression is applicable regardless of frontiers and through any media of one's choice. Res. 69/166 refers to the need to conduct surveillance activities in the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory; and Res. 26/13 alludes to the need to promote digital literacy and bridge the digital divide. Furthermore, Res. 69/166 calls on States to establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data, and to provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy.

The approach taken in the aforementioned resolutions is based on a *normative equivalence paradigm*, which equates the respect, protection and promotion of off-line rights with the respect, protection and promotion of on-line rights. According to this approach, the digital, global and technologically innovative environment in which on-line rights operate represent a challenging (yet, at times, also promising) context for the interpretation and application of off-line rights, which requires the development of new policies, but do not require a re-evaluation of the contents of the rights themselves. In the same manner, the resolutions embrace an *institutional equivalence paradigm*, which equates the role of states vis-a-vis off-line and on-line rights, comprising the facilitation of right enjoyment through securing on-line access, development of right-friendly policies, introduction of legal and institutional safeguards and ensuring access to remedies. The role of private actors is summarily treated in these resolutions: they are stakeholders with which governments should engage, and they incur their own form of corporate social responsibility.

The adequacy of the normative and institutional equivalency approach, however, can be challenged. Arguably, cyber-space creates new needs and interests, as well as new risks, which are not fully captured by existing paradigms. Furthermore, relying primarily on states to cater to such needs and interests and to address new risks does not sit well with the de-territorialized and de-centralized attributes of cyber-space, and the dominant role of non-state actors in constructing this space, regulating it and enforcing rights therein. For example, given the

centrality of social media and other on-line services and platforms in the lives of many individuals, the interest in having on-line access may fast become the on-line equivalent of the right to have rights (or the right to have a legal personality) or even the right to life itself – going much beyond a mere right to receive and impart information. Furthermore, the speed and ease of access to on-line information, and the unlimited duration of its availability, underscores the exceptionally strong interest individuals have in controlling such contents, in limiting third-party access to their personal information, and in obtaining protection from machine-based decision making. It is against this technological and sociological backdrop that some legal systems have started developing new legal rights to informational self-determination[1] (including rights to rectification and erasure), to data portability and to not be subject to decisions based on automatic processing.[2]

The breadth and speed in which on-line data, hardware and software spreads also create new security risks which merit robust protection, which underlies claims for a new right to cyber-security (which is the on-line equivalence of the right to security of person).[3] When the spread of data is combined with the sorting and sifting effects of algorithms governing on-line contents, new risks of manipulation of public opinion and thought control emerge, which may merit a different approach to regulation of speech than has been traditionally the case with off-line speech. Here too, resorting the equivalent normative approach may prove to solve only some problems, while exacerbating others.

Reliance on the institutional equivalence approach might prove to be even more problematic. This is because states currently have only limited ability to exercise a meaningful level of regulatory control over cyber-space, and it might be seriously misguided to encourage them to assume such level of control. As indicated above, the deterritorialized and decentralized attributed of cyber-space, do not sit well with state-by-state regulation. Instead, regulatory efforts should deeply involve IT companies and other stakeholders, and focus on the adherence of their commercial and technological activities, including coding, with relevant international standards, as well as with those self-proclaimed standards and contractual arrangements (such as terms of use) to which they agreed to adhere. In this multi-stakeholder institutional configuration, international coordination and standard setting, and state application of such

[1] BVerfGE 65,1 – Volkszählung.
[2] Regulation (EU) 2016/679 (General Data Protection Regulation), Ch. 3.
[3] ICCPR, art. 9.

standards, plays an important role, albeit complementary in nature. The approach taken in the GA and HR Council resolutions, which focuses mostly on the responsibilities of states, not private actors, is unlikely to offer on-line rights adequate protection.

To be clear, the normative and institutional equivalence approaches do provide in certain cases an appropriate framework for respecting, protecting and promoting rights – for example, states should indeed apply criminal sanctions against individuals who are subject to their jurisdiction involved in child pornography, and should introduce standards to regulate on-line databases administered from their territory. Alas such territorialized cases are becoming exceptional in nature, and even in these rare cases, cooperation by non-state actors in detecting the violation, attributing it to its actual source, sanctioning and remedying it, and preventing its future repetition is indispensable.

2. Specific comments on privacy

The UN Human Rights Committee has reviewed in numerous country reviews under the ICCPR existing on-line surveillance legislation and policies. Several shortcomings have been repeatedly identified by the Committee:

- Lack of Predictability – In a number of countries there is no clear legal basis for the application of surveillance power,[4] or lack of specificity and transparency of the governing legal framework;[5]

[4] HRC Concluding Observations: Namibia (2016)("The Committee notes with concern that interception centres seem operational despite the fact that their legal basis, part 6 of the Communications Act (Act No. 8 of 2009), is not yet in force"); HRC Concluding Observations: Republic of Korea (2015)("It is also concerned about the use and **insufficient regulation** in practice of base station investigations of mobile telephone signals picked up near the site of demonstrations in order to identify participants, and about the extensive use and **insufficient regulation** in practice of wiretapping, in particular by the National Intelligence Service"); HRC Concluding Observations: Italy (2017)("The Committee is concerned about reports that intelligence agencies are intercepting personal communications and employing hacking techniques **without explicit statutory authorization** or clearly defined safeguards from abuse"); HRC Concluding Observations: Turkmenistan (2017)("The Committee is concerned about the lack of a clear legal framework regulating surveillance activities, including by the intelligence services").

[5] HRC Concluding Observations: USA (2014)("The Committee is concerned that, until recently, judicial interpretations of FISA and rulings of the Foreign Intelligence Surveillance Court (FISC) had largely been **kept secret**, thus not allowing affected persons to know the law with **sufficient precision**"); HRC Concluding Observations: France (2015)("The Committee is particularly concerned about the fact that the law on intelligence adopted on 24 June 2015 (submitted to the Constitutional Court) gives the intelligence agencies excessively broad, highly intrusive surveillance powers **on the basis of broad and insufficiently defined objectives**, without the prior authorization of a judge and without an adequate and independent oversight mechanism"); HRC Concluding Observations: Namibia (2016)("While noting the indication by the delegation that all interceptions must be authorized by a magistrate, and that no private information is kept, the Committee is concerned about the **lack of clarity regarding the reach of legal interception possibilities**, as well as about the safeguards to ensure respect of the right to privacy in line with the Covenant"); HRC Concluding Observations: New Zealand (2016)("The Committee is also concerned about the **absence of a clear definition** of the terms "national security" and "private

- Procedural fairness – Privacy standards are applied in some countries in an inconsistent manner, distinguishing, for example, without good reason between nationals and non-nationals, and domestic and foreign collection of data;[6]

communication" in the Telecommunications (Interception Capability and Security) Act 2013"); HRC Concluding Observations: Sweden (2016)("While acknowledging the number of safeguards in place to prevent abuse in the application of the Signals Intelligence Act (2008:717), the Committee remains concerned about the **limited degree of transparency** with regard to the scope of such surveillance powers and the safeguards on their application"); HRC Concluding Observations: Morocco (2016)("The Committee is also concerned by the **lack of clarity** with regard to the legal provisions which authorize and govern surveillance activities"); HRC Concluding Observations: Switzerland (2017): (" the Committee is concerned that this law grants very intrusive surveillance powers to the Confederation's intelligence services on the basis of **insufficiently defined objectives** such as the national interest, referred to in article 3. It is also concerned that the **time period** for which data may be retained is **not specified**").

[6] HRC Concluding Observations: UK (2015)("The Committee is concerned: (a) that the Regulation of Investigatory Powers Act 2000 (RIPA), that makes a distinction between "internal" and "external" communications, provides for untargeted warrants for the interception of external private communication and communication data which are sent or received outside the United Kingdom **without affording the same safeguards** as in the case of interception of internal communications"); HRC Concluding Observations: New Zealand (2016)("The Committee is further concerned about the **limited** judicial authorization process for the interception of communications of New Zealanders and the **total absence** of such authorization for the interception of communications of non-New Zealanders").

- Excessive use of surveillance powers – Some countries have laws affording sweeping data or metadata collection powers,[7] in other countries, there are indications of *de-facto* excesses in the application of surveillance powers;[8]

[7] HRC Concluding Observations: Sweden (2009)("While understanding that security requirements may be aimed at preventing violence and terrorism, the Committee takes note that the Law on Signals Intelligence in Defence Operations (2008:717), will apparently provide the executive with **wide powers** of surveillance in respect of electronic communications"); HRC Concluding Observations: USA (2014)(The Committee is concerned about the surveillance of communications in the interest of protecting national security, conducted by the National Security Agency (NSA) both within and outside the United States, through the **bulk phone metadata** surveillance programme (Section 215 of the USA PATRIOT Act) and, in particular, surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendment Act, conducted through PRISM (collection of communications content from United States-based Internet companies) and UPSTREAM (collection of communications metadata and content by tapping fiber-optic cables carrying Internet traffic) and the adverse impact on individuals' right to privacy"); HRC Concluding Observations: UK (2015)("The Committee is concerned that the State party's current legal regime governing the interception of communications and communication data allows for **mass interception** of communications… The Committee is further concerned that the 2014 Data Retention Investigatory Powers Act provides for **wide powers of retention** of communication data and access to such data does not appear to be limited to the most serious crimes"); HRC Concluding Observations: Canada (2015)(" However, the Committee is concerned about information according to which (a) Bill C-51's amendments to the Canadian Security Intelligence Act confer a broad mandate and powers on the Canadian Security Intelligence Service to act domestically and abroad, thus potentially resulting in **mass surveillance** and targeting activities that are protected under the Covenant without sufficient and clear legal safeguards; (b) Bill C-51 creates, under the Security of Canada Information Sharing Act, an increased sharing of information among federal government agencies on the basis of a very broad definition of activities that undermine the security of Canada, which **does not fully prevent that inaccurate or irrelevant information is shared**"); HRC Concluding Observations: France (2015) ("The Committee is particularly concerned about the fact that the law on intelligence adopted on 24 June 2015 (submitted to the Constitutional Court) gives the intelligence agencies **excessively broad, highly intrusive** surveillance powers on the basis of broad and insufficiently defined objectives, without the prior authorization of a judge and without an adequate and independent oversight mechanism"); HRC Concluding Observations: South Africa (2016) ("The Committee is concerned about the relatively **low threshold** for conducting surveillance in the State party and the relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy contained in the 2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act. It is also concerned about the **wide scope** of the data retention regime under the Act"); HRC Concluding Observations: Denmark (2016) ("In particular, the Committee is concerned about: […] (b) section 780 of the Administration of Justice Act, which allows interception of communication by the police domestically and which may result in **mass surveillance**, despite the legal guarantees provided in sections 781 and 783 of the same Act"); HRC Concluding Observations: Colombia (2016) ("It is also concerned by the fact that the new Police Code that is to enter into force in 2017 defines the concept of "public areas" in **a very broad sense** that includes the electromagnetic spectrum, and by the fact that all the information and data gathered in public areas are considered to be in the public domain and to be freely accessible"); HRC Concluding Observations: Poland (2016) ("The Committee is concerned about the surveillance and interception powers of the Polish intelligence and law enforcement authorities, as reflected in the law on counter-terrorism of June 2016 and the act amending the Police Act and certain other acts of January 2016. The Committee is particularly concerned about: (a) the unlimited and indiscriminate surveillance of communications and collection of metadata"); HRC Concluding Observations: Italy (2016) ("It is also concerned that the anti-terrorism decree and Law No. 21/2016 compel telecommunications service providers to **retain data beyond the period allowed** by article 132 of the personal data protection code, and that the authorities can access such data without authorization from a judicial authority"); HRC Concluding Observations: Pakistan (2017)(" the Committee is concerned that the Act provides for: (a) **overbroad powers** for the Pakistan Telecommunication Authority and authorized officers without sufficient independent judicial oversight mechanisms").

[8] HRC Concluding Observations: UK (2015) ("It notes, inter alia, reports that Amnesty International's email communication had been intercepted by the government under a general warrant"); [8] HRC Concluding Observations: Republic of Korea (2015)("It is also concerned about the use and insufficient regulation in practice of base station investigations of mobile telephone signals picked up near the site of demonstrations in order to **identify participants**, and about the **extensive use** and insufficient regulation in practice of wiretapping, in particular by the National Intelligence Service"); HRC Concluding Observations: South Africa (2016)("The Committee is further concerned at reports of unlawful surveillance practices, including **mass interception** of

- Lack of adequate safeguards – In several countries, there appear to be shortcomings in the existing institutional and normative right protecting mechanisms.[9]

---

communications carried out by the National Communications Centre"); HRC Concluding Observations: Morocco (2016) ("The Committee is concerned by reports of illegal infringements of the right to privacy in the course of surveillance operations conducted by law enforcement and intelligence agencies targeting **journalists, human rights defenders and perceived opponents of the Government**, particularly those located in Western Sahara"); HRC Concluding Observations: Honduras (2017)(" The Committee is concerned at reports of the frequent recourse to the Special Act on Interception of Private Communications, which entails extensive monitoring of private communications"); HRC Concluding Observations: Pakistan (2017)(" the Committee is concerned that the Act provides for:… (b) mandatory mass retention of traffic data by service providers for a minimum of one year"), HRC Concluding Observations: Australia (2017)(" the Committee is concerned about the lack of judicial authorisation for access to such metadata and its **extensive use** in national security, including counterterrorism, and criminal investigations").

[9] HRC Concluding Observations: USA (2014)("The Committee is concerned that the current **oversight** system of the activities of the NSA **fails** to effectively protect the rights of the persons affected; Finally, the Committee is concerned that the persons affected have no access to **effective remedies** in case of abuse"); HRC Concluding Observations: UK (2015)("The Committee is concerned that the State party's current legal regime governing the interception of communications and communication data… lacks sufficient safeguards against arbitrary interference with the right to privacy… The Committee is concerned: … (b) about the **lack of sufficient safeguards** for obtaining private communications from foreign security agencies and for sharing personal communications data with such agencies"); HRC Concluding Observations: Canada (2015)("However, the Committee is concerned about information according to which (a) Bill C-51's amendments to the Canadian Security Intelligence Act confer a broad mandate and powers on the Canadian Security Intelligence Service to act domestically and abroad, thus potentially resulting in mass surveillance and targeting activities that are protected under the Covenant **without sufficient and clear legal safeguards;** The Committee is also concerned about the **lack of adequate and effective oversight** mechanisms to review activities of security and intelligence agencies, and the **lack of resources and power** of existing mechanisms to monitor such activities"); HRC Concluding Observations: France (2015)("The Committee is particularly concerned about the fact that the law on intelligence adopted on 24 June 2015 (submitted to the Constitutional Court) gives the intelligence agencies excessively broad, highly intrusive surveillance powers on the basis of broad and insufficiently defined objectives, **without the prior authorization of a judge and without an adequate and independent oversight mechanism**"); HRC Concluding Observations: Republic of Korea (2015)("The Committee notes with concern that, under article 83 (3) of the Telecommunications Business Act, subscriber information may be requested **without a warrant** by any telecommunications operator for investigatory purposes"); HRC Concluding Observations: Namibia (2016)("While noting the indication by the delegation that all interceptions must be authorized by a magistrate, and that no private information is kept, the Committee is concerned about the lack of clarity regarding the reach of legal interception possibilities, as well as about the **safeguards** to ensure respect of the right to privacy in line with the Covenant"); HRC Concluding Observations: New Zealand (2016)("The Committee is further concerned about the **limited judicial authorization** process for the interception of communications of New Zealanders and the **total absence** of such authorization for the interception of communications of non-New Zealanders"); HRC Concluding Observations: Rwanda (2016)("The Committee is concerned that Law No. 60/2013 permits the interception of communications **without prior authorization of a judge");** HRC Concluding Observations: Sweden (2016)("While acknowledging the number of safeguards in place to prevent abuse in the application of the Signals Intelligence Act (2008:717), the Committee remains concerned about the **limited degree of** transparency with regard to the scope of such surveillance powers and the **safeguards** on their application"); HRC Concluding Observations: South Africa (2016)("The Committee is concerned about the relatively low threshold for conducting surveillance in the State party and the **relatively weak safeguards, oversight and remedies** against unlawful interference with the right to privacy contained in the 2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act… The Committee is further concerned at… delays in fully operationalizing the Protection of Personal Information Act, 2013, due in particular to **delays in the establishment of an information regulator**"); HRC Concluding Observations: Colombia (2016)("The Committee is also concerned that the "electromagnetic spectrum monitoring" provided for in article 17 of Act No. 1621 of 2013 could result in instances in which private communications conveyed via the electromagnetic spectrum are intercepted **without the benefit of a rigorous assessment** of the legality, necessity and proportionality of such interceptions"); HRC Concluding Observations: Morocco (2016) ("The Committee is also concerned by the lack of clarity with regard to the legal provisions which authorize and govern surveillance activities and the **lack of oversight** of those activities by an **independent authority**"); HRC Concluding

Responding to these shortcoming, the Committee has issued some specific recommendations, aimed at ensuring the equal application of privacy protections to all individuals subject to the jurisdiction of the state,[10] enhancing the specificity and transparency of surveillance laws,[11] narrowing surveillance powers, so as to ensure close tailoring of powers to needs,[12] and

---

Observations: Italy (2017)("The Committee is concerned about reports that intelligence agencies are intercepting personal communications and employing hacking techniques without explicit statutory authorization or **clearly defined safeguards from abuse**. It is also concerned that the anti-terrorism decree and Law No. 21/2016 compel telecommunications service providers to retain data beyond the period allowed by article 132 of the personal data protection code, and that the authorities can access such data **without authorization from a judicial authority**"); HRC Concluding Observations: Honduras (2017) ("the Committee regrets the lack of sufficient information on the grounds and evidence needed to obtain judicial authorization for surveillance operations, the **absence of appropriate oversight mechanisms** to continuously monitor the application of the Special Act, and the difficulties of victims of unlawful surveillance to obtain legal redress"); HRC Concluding Observations: Pakistan (2017)(" the Committee is concerned that the Act provides for: (a) overbroad powers for the Pakistan Telecommunication Authority and authorized officers **without sufficient independent judicial oversight mechanisms**"); HRC Concluding Observations: Australia (2017)("the Committee is concerned about the **lack of judicial authorisation for access to such metadata** and its extensive use in national security, including counterterrorism, and criminal investigations").

[10] HRC Concluding Observations: USA (2014)("measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance"); HRC Concluding Observations: UK (2015)("In particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance"); HRC Concluding Observations: New Zealand (2016)("Sufficient judicial safeguards are implemented, **regardless of the nationality or location** of affected persons, in terms of interception of communications and metadata collection, processing and sharing").

[11] HRC Concluding Observations: USA (2014)("Ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that : (i) are **publicly accessible**;… (iii) are **sufficiently precise and specify in detail** the precise circumstances in which any such interference may be permitted , the procedures for authorization , the categories of persons who may be placed under surveillance , the limit on the duration of surveillance; procedures for the use and storage of data collected"); HRC Concluding Observations: UK (2015)("Ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that: (i) are **publicly accessible**… (iii) are **sufficiently precise and specify in detail** the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance; procedures for the use and storage of data collected"); HRC Concluding Observations: France (2015)("The State party should ensure that the collection and use of data on communications take place on the basis of specific and legitimate objectives and that the **exact circumstances** in which such interference may be authorized and the categories of persons likely to be placed under surveillance are **set out in detail**"); HRC Concluding Observations: South Africa (2016)("It should also ensure that interception of communications by law enforcement and security services is carried out **only according to the law** and under judicial supervision"); HRC Concluding Observations: Sweden (2016)("The State party should **increase the transparency** of the powers of and safeguards on the National Defence Radio Establishment, the Foreign Intelligence Court and the Data Inspection Board, by considering to make their **policy guidelines and decisions public,** in full or in part, subject to national security considerations and the privacy interests of individuals concerned by those decisions"); HRC Concluding Observations: Turkmenistan (2017)("The State party should ensure that: (a) all types of surveillance activities and interference with privacy, including online surveillance for the purposes of State security**, are governed by appropriate legislation** that is in full conformity with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity, and that State practice conforms thereto").

[12] HRC Concluding Observations: UK (2015)("Ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that:… (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; Revise the 2014 Data Retention Investigatory Powers Act with a view to ensuring that access to communication data is limited to the extent strictly necessary for the prosecution of the most serious crimes and dependent upon prior judicial authorization"); HRC Concluding Observations: France (2015)("The State party should ensure that the collection and use of data on communications take place on the basis of **specific and legitimate objectives** and that the exact circumstances in

developing effective safeguards, which include, when appropriate, judicial involvement, remedies for individuals subject to unlawful surveillance operations, and independent monitoring over the application of all on-line surveillance powers.[13] One specific element that

which such interference may be authorized and the categories of persons likely to be placed under surveillance are set out in detail"); . HRC Concluding Observations: Rwanda (2016)(" It should also ensure that communications are intercepted and data are used to achieve **specific and legitimate objectives** and that the categories of circumstances in which such interference may be authorized and the categories of persons whose communications are likely to be intercepted are set out in detail"); HRC Concluding Observations: Namibia (2016)("The State party should ensure that the interception of telecommunications may only be **justified under limited circumstances** authorized by law with the necessary procedural and judicial safeguards against abuse, and supervised by the courts when in full conformity with the Covenant").

[13] HRC Concluding Observations: Sweden (2009) ("The State party should take all appropriate measures to ensure that the gathering, storage and use of personal data not be subject to any abuses, not be used for purposes contrary to the Covenant, and be consistent with obligations under article 17 of the Covenant. To that effect, the State party should guarantee that the processing and gathering of information be subject to **review and supervision by an independent body with the necessary guarantees of impartiality and effectiveness**"); HRC Concluding Observations: USA (2014)("Ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that:… (iv) provide for effective safeguards against abuse; (c) Reform the current oversight system of surveillance activities to ensure its effectiveness, including by providing for **judicial involvement** in the authorization or monitoring of surveillance measures, and considering the establishment of strong and **independent oversight mandates** with a view to preventing abuses;… (e) Ensure that affected persons have access to **effective remedies** in cases of abuse"); HRC Concluding Observations: UK (2015)("Ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that:… (iv) provide for effective safeguards against abuse; Ensure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by providing for **judicial involvement** in the authorization of such measures in all cases, and considering the establishment of **strong and independent** oversight mandates with a view to preventing abuses; Ensure that affected persons have access to effective remedies in cases of abuse"); HRC Concluding Observations: France (2015)("It should also ensure the effectiveness and independence of a monitoring system for surveillance activities, in particular by making provision for the **judiciary to take part** in the authorization and monitoring of surveillance measures"); HRC Concluding Observations: Canada (2015)("establish oversight mechanisms over security and intelligence agencies that are effective and adequate, and provide them with **appropriate powers** as well as **sufficient resources** to carry out their mandate; provide for **judicial involvement** in the authorization of surveillance measures"); HRC Concluding Observations: Republic of Korea (2015)("It should, inter alia, ensure that subscriber information may be issued with a **warrant** only, introduce a **mechanism to monitor** the communication investigations of the National Intelligence Service, and increase the **safeguards** to prevent the arbitrary operation of base station investigations"); HRC Concluding Observations: Sweden (2016)("It should ensure:… (b) that **effective and independent oversight mechanisms** over intelligence-sharing of personal data are put in place; and (c) that affected persons have proper access to **effective remedies** in cases of abuse"); HRC Concluding Observations: Rwanda (2016)("It should also ensure the **effectiveness and independence** of a **monitoring system** for such interception , in particular by providing for the **judiciary** to take part in the authorization and monitoring of the interception"); HRC Concluding Observations: Namibia (2016)("The State party should ensure that the interception of telecommunications may only be justified under limited circumstances authorized by law with the necessary procedural and judicial **safeguards** against abuse, and **supervised by the courts** when in full conformity with the Covenant"); HRC Concluding Observations: New Zealand (2016)("**Sufficient judicial safeguards** are implemented, regardless of the nationality or location of affected persons, in terms of interception of communications and metadata collection, processing and sharing"); HRC Concluding Observations: South Africa (2016)("The State party should refrain from engaging in mass surveillance of private communications without prior **judicial authorization**… It should also ensure that interception of communications by law enforcement and security services is carried out only according to the law and **under judicial supervision**"); HRC Concluding Observations: Morocco (2016)("The State party should also establish **independent oversight mechanism**s in order to prevent abuses"); HRC Concluding Observations: Italy (2017)("The State party should review the regime regulating the interception of personal communications, the hacking of digital devices and the retention of communications data with a view to ensuring: … (b) that **robust, independent oversight systems** are in place regarding surveillance, interception and hacking, including by ensuring that the **judiciary is involved** in the authorization of such measures, in all cases, and by affording persons affected with **effective remedies in cases of abuse**, including, where possible, an **ex post notification** that they were placed under surveillance or

had been raised in the context of the some review processes had been the need to strictly limit any mandatory retention period imposed on third parties.[14]

Future developments in the field of regulating on-line surveillance may include the emergence of a duty for *ex post facto* notification of persons who were under surveillance (subject to exceptional security considerations), in order to facilitate the attainment of effective remedies, the development of more specific criteria for evaluating the adequacy of judicial and non-judicial safeguards (such as the attributes and powers of independent ombudsmen or privacy commissioners, akin to standards developed for national human rights institutions) and the representation of privacy interests in judicial or quasi-judicial surveillance authorization procedures (through special advocates or privacy commissioners). More work is also needed on new standards for the regulation of technology development and transfers, and intelligence sharing.[15] Such new standards should apply to state and non-state actors.

3. Specific comments on other rights

No doubt, the internet plays an increasingly important role in the lives of individuals, and constitutes a key space in which rights, such as the freedom of receive and impart information, freedom of expression and right to political participation, the right to education, are being increasingly realized. Furthermore, as indicated above, the unique attributes of cyber-space may encourage the creation of new rights and legal personalities worthy of protection (which

---

that their data was hacked"); HRC Concluding Observations: Turkmenistan (2017)("The State party should ensure that: … (b) surveillance is subject to **judicial authorization** as well as **effective** and **independent oversight m**echanisms; and (c) affected persons have proper access to **effective remedies** in cases of abuse"); HRC Concluding Observations: Honduras (2017)("The State party should also ensure that the application of the Special Act on Interception of Private Communications is subject to continuous and appropriate monitoring through an **independent oversight mechanism** and that it provides victims with **appropriate remedies**").

[14] HRC Concluding Observations: USA (2014) ("Refrain from imposing mandatory retention of data by third parties"); HRC Concluding Observations: South Africa (2016) ("The State party should… consider revoking or limiting the requirement for mandatory retention of data by third parties"); HRC Concluding Observations: Pakistan (2017)("It should… review all licensing requirements that impose obligations on network service providers to engage in communication surveillance, particularly in relation to indiscriminate data retention").

[15] HRC Concluding Observations: Sweden (2016) ("It should ensure: (a) that all laws and policies regulating the **intelligence-sharing of personal data** are in full conformity with its obligations under the Covenant; that effective and independent oversight mechanisms over intelligence-sharing of personal data are put in place"); HRC Concluding Observations: Pakistan (2017)(" It should also… review its laws and practice of intelligence-sharing with foreign agencies to ensure its compliance with the Covenant"); HRC Concluding Observations: Switzerland (2017)("In particular, measures should be taken to ensure that the time limits for data retention are **strictly regulated**").

.

may be regarded as the on-line avatars of off-line persons); this environment also introduces new risks to traditional and digital rights.

It is critical for relevant stake holders – including, states, IT companies, international organizations, on-line communities - to cooperate in preserving critical aspects of the internet that are conducive for promoting human rights therein: primarily, net neutrality and open and equal access to the web. Global and interoperable access to on-line data and services that is affordable, and a critical mass of free on-line contents are other important conditions for enjoyment of rights in cyber-space.

Furthermore, relevant stakeholders should develop suitable procedures for addressing potential right-infringements, such as notify-and-remove procedures for harmful speech, as defined in article 20 of the ICCPR, right to rectification of false information, and a legal process for challenging decisions relating to on-line access, participation in on-line communities, and other rights of data subjects.

Finally, relevant stakeholders ought to undertake measures necessary for protecting cyber-space as an arena in which civil and political rights can be meaningfully realized, which go over and beyond cyber-security, and law-enforcement (e.g., detection, attribution and sanctioning) against human rights abusers. These include measures designed to increase the transparency of on-line publications (especially of organized efforts to publish contents), to label or provide other tools to detect patently fraudulent information (such as fake news), to open-up hermetically sealed echo-chambers which significantly impact the shape of political discourse and to actively promote awareness to human rights norms, through facilitating access to information about human rights violations and relevant on-line right protecting mechanisms, such as compliance or corporate social responsibility offices, and privacy or IT ombudsmen.