10th Internet Governance Forum – November 2015

RECOMMENDATIONS ON TERMS OF SERVICE & HUMAN RIGHTS

Introduction

The following recommendations aim at fostering online platforms' responsibility to respect human rights, in accordance with the UN Guiding Principles on Business and Human Rights, by providing guidance for "responsible" terms of service. For the purpose of these recommendations, the term "responsible" should be understood as respectful of internationally agreed human rights standards. Besides identifying minimum standards for the respect of human rights by platform operators (standards that "**shall**" be met), these recommendations suggest best practices (which are "**recommended**", or "**should**" be followed) for the most "responsible" adherence to human rights principles in the drafting of terms of service.

Background

The digital environment is characterized by ubiquitous intermediation: most of the actions we take on the web are enabled, controlled or otherwise regulated through the operation of online platforms (see: definition n in Appendix 1). Online platforms are essential instruments for individuals to educate themselves, communicate information, store and share data (see definition d in Appendix). Increasingly, the operation of these platforms affects individuals' ability to develop their own personality and engage in a substantial amount of social interactions. The online world might thus challenge the system of human rights protection traditionally used in the offline world, which relies predominantly on a public infrastructure. While private actors are traditionally not considered as duty-bearers in international human rights law, they are indirectly subject to international law through the laws of the countries in which they operate. However, since national laws do not always adequately implement internationally-agreed human rights, there is a need to define minimum standards and develop voluntary best practices at the international level to ensure protection of human rights by transnational corporations.

Respect of human rights undoubtedly represents an important factor in assessing the conduct of corporations from the perspective of a variety of stakeholders, including governments, investors and increasingly, consumers. This is especially relevant in the context of online platforms designed to serve the needs of a global community, and forced to satisfy different, often conflicting legal requirements across the various jurisdictions where they operate. In light of the key role that online platforms are playing in shaping a global information society and the significant impact they have on the exercise of the rights of Internet users (see definition k in Appendix), an expectation exists that such entities behave "responsibly", thus refraining from the violation of internationally recognised human rights standards and offering effective remedies aimed at repairing the negative consequences that their activities may have on users' rights.[1]

The existence of a responsibility of private sector actors to respect human rights, which was affirmed in the UN Guiding Principles on Business and Human Rights[2] and unanimously endorsed by the UN Human Rights Council, is grounded upon the tripartite framework developed by the UN Special Rapporteur for Business and Human Rights, according to which States are the primary duty bearers in securing the protection of human rights, corporations have the responsibility to respect human rights, and both entities are joint duty holders in providing effective remedies against human rights violations.

As part of this responsibility, corporations should:

1. make a policy commitment to the respect of human rights
2. adopt a human rights due-diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights; and
3. have in place processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute[3].

These recommendations focus on one of the most concrete and tangible means for online platforms to bring that responsibility to bear: the contractual agreement which Internet users are required to adhere to in order to utilise their services (usually called "Terms of Service", see definition s in appendix 1). Specifically, the recommendations constitute an attempt to define "due diligence" standards for online platforms with regard to **three essential components: privacy, freedom of expression and due process**. In doing so, they aim to provide a benchmark for respect of human rights, both in the relation of a platform's own conduct as well as with regard to the scrutiny of governmental requests that they receive. As recently stressed by the Council of Europe's Commissioner for Human

Rights[4], guidance on these matters is particularly important due to the current lack of clear standards.

I. Privacy & Data Protection (see definition q in Appendix)

The first section of these recommendations provides guidance over the rules that online platform operators (see definition o in Appendix) can adopt in order to guarantee that their users are not subject to unnecessary or unreasonable collection, use and disclosure of their personal data (see definition m in Appendix).

1. Data Collection

Platform operators **should** limit the collection of personal information (see definition m in Appendix) from Internet users to what is directly relevant and necessary to accomplish a specific, clearly defined and explicitly communicated purpose[5]. The platform's terms of service (ToS) **shall** also specify every type or category of information collected, rather than requiring a general-purpose consent (see definition c in Appendix)[6]. If consent is withdrawn, the platform is no longer entitled to process such data for the related purpose. Although withdrawal is not retroactive, *i.e.* it cannot invalidate the data processing that took place in the period during which the data was collected and retained legitimately, it **shall** prevent any further processing of the individual's data by the controller and should imply deletion unless further use is permitted and regulated by a legitimate law (see definition l in Appendix)[7].

Platform operators **shall** also refrain from collecting data by automatically scanning content (see definition b in Appendix) privately shared by their users, in the absence of platform-users' consent. Admissible derogations to this principle include the need to fight against unsolicited communications (spam), maintain network security (e.g. preventing the diffusion of malware) or give force to court order or provisions defined by a legitimate law.

Platform operators **shall** always obtain user consent before tracking their behaviour (both within the platform and outside, *e.g*. through social plugins on third-party sites). Even after consent has been given, they **shall** always provide a way for users to opt-out at a later stage by the platform within other services. In order to facilitate user oversight on the application of these principles, platform operators **shall** allow their users to view, copy, modify and delete the personal information they have made available to the platform, both within its own services or by other services within the platform, and are encouraged to do so enabling download of a copy of their personal data (see definition m in Appendix) in

interoperable format[8]. Platform operators **shall** also allow their users to view, modify and delete the personal information that platform operators have shared with third parties for marketing purposes.

2. **Data Retention**

Platform operators **should** clearly communicate in their terms of service whether and for how long they are storing any personal data. As a general rule, any retention beyond the period necessary to accomplish the purpose (not exceeding 180 days)[9] **should** be specifically foreseen by a "legitimate law"[10].

3. **Data aggregation**

As a best practice, aggregation of platform users' data **should** only be done subject to express consent (see definition g in Appendix). Aggregation of data across multiple services or devices requires extra diligence from the part of the data controller (see definition e of Annex 1), since it might result in data being processed beyond the original purpose for which it was collected and the generation of new data, whose nature, volume and significance may nor be known or knowable by the platform user (see definition p in Appendix). The purpose of the data aggregation and the nature of the new data resulting from the aggregation **should** be clearly stated, in order to allow the platform users to properly understand the scope of the given consent. Although this does not prevent the implementation of cross-device functionalities[11], it is necessary to ensure that platform users understand the reason, scope and outputs of the data aggregation.

4. **Data Use**

Platforms **shall** obtain consent in order to use personal data (including platform users' contacts and recipients) for the legitimate purpose and duration as specified within the Terms of Service. Additional use of platform user's personal data does not require the platform user' consent when such use is necessary: (a) for compliance with a legal obligation to which the platform operator is subject; or (b) in order to protect the vital interests or the physical integrity of the platform user or of a third person; (c) for the performance of a task carried out in the public interest or in the exercise of official authority as specified by a legitimate law. (d) for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject [12] . However, express consent **should** be required for making

personal data available to the public. Platform users **should** have the possibility to redefine the extent to which their personal data are available to the public.

A broad and open-ended permission on the use of platform users' personal data for "future services"[13] can be in conflict with the right of users to informational self-determination[14]. For this reason, it **is recommended** that platforms specify in their ToS that the processing of personal data is limited to the scope of existing services, or explicitly state that the data can be used for specified additional services. The enrolment of platform users into any new service shall require the acceptance of new ToS.

Platform operators shall also give users the possibility to demand the rectification of inaccurate data and to object to the use of their personal data on legitimate grounds, unless such use is mandated by a legitimate law [16]. Furthermore, platform users **shall** always be able to obtain information about any predictive or probabilistic techniques that have been used to profile them and the underlying rationale of such profiling[17].

Lastly, platform operators **shall** always permit their users to delete their account in a permanent fashion[18]. Likewise, if there is no other legal reason justifying the further storage of the data, the data processor shall proceed with the permanent deletion of all or portions of the relevant data associated with the platform user's account[19], in a time that is reasonable for its technical implementation. While anonymous data (see definition a in Appendix) can be kept and processed without consent, pseudonymous data (see definition r in Appendix) should not be subject to different treatment in that regard.

5. **Data protection** *vis-à-vis* **third parties**

Platform operators **shall** provide effective remedies against the violation of internationally recognised human rights. For this reason, they **should** establish clear mechanisms for platform users to gain access to all of their personal data held by a third party to whom their data have been transferred, as well as to be informed of the actual usage thereof[20]. Platform operators **should** also enable their users to report privacy-offending content and to submit takedown requests[21]. When such requests are submitted, a balance of the relevant rights and interests should be made and the outcome may depend on the nature and sensitivity of the privacy-offending content and on the interest of the public in having access to that particular information[22]. They **should** also implement a system to prevent the impersonation of platform users by third parties, although exceptions can be made with regard to public figures where pertinent to contribute to the public debate in a democratic society[23].

A second set of concerns pertains to the possibility to preempt any interference with platform users' personal data, by preventing third parties' access to platform user's content and metadata. Firstly, platform operators **should** allow users to preserve their anonymity *vis-à-vis* third parties to the extent permitted by legitimate laws. Secondly, it is **recommended** that platforms enable end-to-end encryption of communications and other personal information, in the context of both storage and transmission[24]. In that respect, **best practice** is when the decryption key is retained by the platform user, except where the provider needs to hold the decryption key in order to provide the service and the platform user has provided informed consent.

As regards the handing over of platform users' data upon governmental request, platform operators **should** specify that they execute such request only in the presence of a valid form of legal process, and release a periodic transparency report providing, per each jurisdiction in which they operate, the amount and type of such requests, and the platforms' response (in aggregate numbers).[25]

II. Due Process

Due process (see definition f in Appendix) is a fundamental requirement for any legal system based on the rule of law. "Due" process refers to the non-derogability of certain procedures in situations which may adversely affect individuals within the legal system. These procedures are grounded upon essential principles such as the clarity and predictability of the substantive law, the right to an effective remedy against any human rights violations and the right to be heard before any potentially adverse decision is taken regarding oneself. In particular, while a law must be clear and accessible to the platform user, the latter principles translate into the need for an appeal system and the respect of the core minimum of the right to be heard, including: (1) a form of legal process which respects the guarantees of independence and impartiality; (2) the right to receive notice of the allegations and the basic evidence in support, and comment upon them, to the extent that not doing so may prejudice the outcome of the dispute; and (3) the right to a reasoned decision.

Due process has significant implications with regards to potential amendment and termination of contractual agreements, as well as the adjudication of potential disputes.

1. Amendment and termination of contracts

Terms of Service **should** be written in plain language that is easy to understand. The platform operators should provide an accessible summary of the key provisions of the

terms of service. The platform operators **should** give their users meaningful notice of any amendment of the ToS affecting the rights and obligation of the users. Meaningful notice **should** be provided in a way, format and timing that enable platform users to see, process and understand the changes without unreasonable effort. Contractual clauses that permit termination by platforms without clear and meaningful notice **shall** not be used.

In addition, platform operators **should** consider giving notice even of less significant changes, and enabling their users to access previous versions of the terms of service. Ideally, platforms operators **should** enable their users to continue using the platform without having to accept the new terms of service related to the additional functionalities. Additional functionalities should never be imposed to the user when it is possible to provide the original service without implementing the additional functionalities. The platform user should have the possibility to opt in in for new functionalities. Meaningful notice **should** also be given prior to termination of the contract or services. Besides, to reduce the imbalance between platform users and platforms owners when it comes to litigation, it is **recommendable** that the ToS be negotiated beforehand with consumer associations or other organisations representing Internet users. In order to prevent wrongful decisions, it is **also recommended** that platforms make termination of accounts of particular platform users possible only upon repeated violation of ToS or on the basis of a court order.

2. **Adjudication**

Disputes can arise both between platform users and between a particular platform user and the platform operator. In both cases, platform operators **should** provide alternative dispute resolutions systems to allow for quicker and potentially more granular solutions than litigation for the settling of disputes. However, in view of the fundamental importance of the right of access to court, alternative dispute resolution systems **should** not be presented as a replacement of regular court proceedings, but only as an additional remedy. In particular, platform operators **should** not impose waiver of class action rights or other hindrances to the right of an effective access to justice, such as mandatory jurisdiction outside the place of residence of Internet users. Any dispute settlement mechanism **should** be clearly explained and offer the possibility of appealing against the final decision.

III. Freedom of Expression

Freedom of expression (see definition h in Appendix) is a fundamental right consisting of the freedom to hold opinions without interference and Freedom of expression may be

subject to certain restrictions that shall be explicitly defined by a legitimate law. In the online platform context, the effectiveness of this right can be seriously undermined by disproportionate monitoring of online speech and repeated government blocking and takedown. The following section provides guidance as to how platforms should handle such matters through their terms of service.

1. **Degree of monitoring**

Although there are no rules to determine, in general terms, what kind of speech should or should not be allowed in private online platforms, certain platforms **should** be seen more as "public spaces" to the extent that occupy an important role in the public sphere.[26] These actors have assumed functions in the production and distribution process of media services which, until recently, had been performed only (or mostly) by traditional media organisations[27]. As a matter of fact, online platforms increasingly play an essential role of *speech enablers* and pathfinders to information, becoming instrumental for media's outreach as well as for Internet users' access to them[28].

As a general rule, any restriction on the kind of content permitted on a particular platform should be clearly stated and communicated within the ToS. In addition, platforms **should** provide effective mechanisms aimed at signalling and requesting the removal of content that is forbidden under the applicable legitimate laws (e.g. illegal content such as child pornography as well as other kinds of undesirable content, such as hate speech, spam or malware). However, such mechanisms shall be necessary and proportionate to their purpose.[29] It is of utmost importance that the rules and procedures imposing such restrictions are not formulated in a way that might affect potentially legitimate content, as they would otherwise constitute a basis for censorship. To this end, content restriction requests pertaining to unlawful content shall specify the legal basis for the assertion that the content is unlawful; the Internet identifier and description of the allegedly unlawful content; and the procedure to be followed in order to challenge the removal of the content [30].

Similarly, although platforms can legitimately remove content that is not allowed by their terms of service, either on their own motion or upon complaint, such terms of service **should** be clear and transparent in their definition of the content that will be restricted within the platform. However, when platforms offer services which have become essential for the enjoyment of fundamental rights in a given country, they should not restrict content beyond the limits defined by the legitimate law. Lastly, **platforms may** legitimately prohibit the use of the name, trademark or likeness of others, when such

use would constitute an infringement of the rights of third parties. However, platforms operator **should** always provide clear mechanisms to notify those platform users whose content has been removed or prohibited and provide them with an opportunity to challenge and override illegitimate restrictions.

2. **Government blocking and takedowns**

Transparent procedures should be adopted for the handling and reporting of governmental requests for blocking and takedown in a way that is consistent with internationally recognised laws and standards.[31] Firstly, platform operators **should** execute such requests only when these are grounded on legitimate law. The content should be permanently removed only when such operation is justified by a judicial order, or the takedown request has not been appealed or countered in due course. Secondly, platforms operators **should** notify their users of such requests, ideally giving them an opportunity to reply and challenge their validity, unless specifically prohibited by a legitimate law. Finally, as already mentioned in the context of government requests for data, platform operators **should** adopt law enforcement guidelines and release periodic transparency reports.

IV. Protection of Children and Young People

A special category of concerns arises in the case of children and young people, towards which platform operators **should** exercise a higher level of care. Platform operators **should** adopt particular arrangements, beyond warning for inappropriate content and age verification that can be imposed by legitimate law for certain types of content.

First, parental consent **should** be required for the processing of personal data of minors, in accordance with the applicable legislation. Secondly, although terms of service **should** generally be drafted in an intelligible fashion, those regulating platforms open to children and young people **should** consider including facilitated language or an educational video-clip and, ideally, a set of standardised badges[32] to make their basic rules comprehensible by all users regardless of their age and willingness to read the actual terms of use[33]. Secondly, **it is recommended** that platforms provide measures that can be taken by children and young people in order to protect themselves while using the platform[34], such as utilising a "safer navigation" mode. Thirdly, platform operators **shall** offer specific mechanisms to report inappropriate content, and **should** providing a mechanism to ensure removal or erasure of content created by children and young people[35].

As an element of media literacy, all platform users **should** be informed about their right to remove incorrect or excessive personal data[36].

Annex 1: Definitions

a) Anonymous data

Anonymous data means personal data processed in such a way that it can no longer be used to identify a natural person by using all the available means likely to be used" by either the controller or a third party.

b) Content:

Text, image, audio or video provided to particular platform user within the platform, even on a transient basis. This includes content produced and/or published by the platform operator, by another platform user or by a third party having a contractual relationship with the platform operator.

c) Consent:

Consent means any freely given, specific, and informed indication of the data subject's wishes by which s/he signifies her/his agreement to personal data relating to her/himself being processed.[37] To that end, every user shall be able to exercise a real choice with no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.

d) Data:

Content and/or personal information. Data can belong to both categories simultaneously.

e) Data controller

Data controller is the institution or body that determines the purposes and means of the processing of personal data

f) Due Process:

Due process is a concept referring to procedural rights which are essential for the respect of the rule of law, comprising: (1) a form of legal process which respects the guarantees of independence and impartiality; (2) the right to receive notice of the allegations and the basic evidence in support, and comment upon them, to the extent that not doing so may prejudice the outcome of the dispute; and (3) the right to a reasoned decision.

g) Express Consent:

Express consent is a type of consent which (in contrast with "implicit" or "implied" consent) requires an affirmative step in addition to the acceptance of the general ToS, such as clicking or ticking a specific box or acceptance of the terms and conditions of a separate document.

h) Freedom of Expression:

The right to freedom of expression, enshrined in article 19 of the International Covenant on Civil and Political Rights consist of the freedom to hold opinions without interference and include freedom to seek, receive and impart information and ideas, regardless of frontiers. Freedom of expression may be subject to certain restrictions that shall be explicitly defined by a legitimate law. The right to freedom of opinion and expression is as much a fundamental right on its own accord as it is an "enabler" of other rights, including economic, social and cultural rights.[38]

i) Function of the Platform:

Function that the community has attributed to the platform on the basis of the legal, commercial and social expectations that it has generated. This should not be confused with a platform's functionalities, which constitute merely one (albeit important) element to identify the overall function(s).

j) Hate Speech:

Although there is no universally accepted definition of "hate speech", the term shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination on any grounds such as race, ethnicity, colour, sex, language, religion, political or other opinion, national or social origin, property, disability, birth, sexual orientation or other status[39]. In this sense, "hate speech" covers comments which are necessarily directed against a person or a particular group of persons[40].

k) Internet User

An individual who is using Internet access service, and in that capacity has the freedom to impart and receive information. The Internet user may be the subscriber, or any person to whom the subscriber has granted the right to use the Internet access service s/he receives.

l) Legitimate Law:

Laws and regulations are procedurally legitimate when they are enacted on the basis of a democratic process. In order to be regarded also as substantively legitimate, they must respond to a pressing social need and, having regard to their impact, they can be considered as proportional to the aim pursued[41].

(a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency);

(b) It must pursue a legitimate purpose (principle of legitimacy)[42]; and

(c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).

If it is manifest that the measure would not pass this three-pronged test, the platform operator should deny the request and, to the extent possible, challenge it before the relevant court.

m) Personal Data & Personal Information:

Personal data is any information about an individual that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, etc.[43] This is not intended to cover identification which can be accomplished via very sophisticated methods[44]. This notion of personal data is sometimes also referred to as Personally Identifiable Information (PII), defined as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[45]

n) Platform:

For the purpose of these recommendations, platforms are understood as any applications allowing users to seek, impart and receive information or ideas according to the rules defined into a contractual agreement.

o) Platform Operator

Natural or legal person defining and having the possibility to amend the platform's terms of service

p) Platform User

Natural or legal person entering into a contractual relationship defined by the platform's terms of service.

q) Privacy & Data Protection:

Privacy is an inalienable human right enshrined in Article 12 of the Universal Declaration of Human Rights, which establishes the right of everyone to be protected against arbitrary interference with their privacy, family, home or correspondence, and against attacks upon his honour and reputation. In the context of online platforms, this encompasses the ability for data subjects to determine the extent to which and the purpose for which their personal data is used by data controllers, including the conditions upon which such data can be processed by the holder of data (the platform) and/or made available to third parties (right to informational self-determination).

r) Pseudonymous Data:

Pseudonymous data means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution

s) Terms of Service:

The concept of "terms of service" utilised here covers not only the contractual document available under the traditional heading of "terms of service" or "terms of use", but also any other platform's policy document (*e.g*. privacy policy, community guidelines, *etc*.) that is linked or referred to therein.

Footnotes

[1] See Council of Europe, Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media

[2] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie: Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, UN Human Rights Council Document A/HRC/17/31, 21 March 2011 {"Guiding Principles"), p. 1

[3] Guiding Principles, Part II, B, para. 15

[4] Council of Europe, "The Rule of Law on the Internet and in the Wider Digital World", footnotes 181-187 and corresponding text.

[5] See Principle I.3 of the OECD Privacy Principles ("The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."); Principle III of the APEC Privacy Framework which " limits collection of information by reference to the purposes for which it is collected. The collection of the information should be relevant to such purposes, and proportionality to the fulfilment of such purposes may be a factor in determining what is relevant"; and Principle 3 of the UN Data Protection Principles and Rights, according to which "The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that: (a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified; (b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified? (c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified.

[6] See Principle III of the OECD Privacy Principles; and Principle 5 of the APEC Privacy Framework.

[7] See Principle UN Data Protection Principle and Rights ("Everyone [...] has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees") and Art. 8e of the modernized version of Convention 108 ("Any person shall be entitled: [...] to obtain, upon request, as the case may be, rectification or erasure of such data"). See also Opinion 15/2011 of the Article 29 Working Party on the definition of consent, p. 9

[8] See article 15 of the proposed EU data protection regulation.

[9] Given the importance of data about past platform user behaviour for the provision of personalised search results, it appears unnecessary, as a matter of principle, to apply data retention periods exceeding those foreseen for search engines. Thus, the criterion of 180 days is based on the recognition by the Article 29 Working Party that search engines do

not need, in principle, to store data for longer than 6 months- beyond which period, retention should be "comprehensively" justified on "strict necessity" grounds. See Art. 29 WP Opinion 1/2008 on data protection issues related to search engines, p. 19

[10] See Annex 1, definition p): "Legitimate Law"

[11] One example of such functionality is the recently added cross-device tracking feature of Google Analytics. See https://support.google.com/analytics/answer/3234673?hl=en

[12] See e.g. art 7, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[13] See e.g. Google's Terms of Services (http://www.google.com/intl/en/policies/terms) stating that "The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop *new* ones" (as of 15 January 2015).

[14] For the development of this principle, see the decision by the German Constitutional Court in the so called "census" decision. BVerfGe 65, 1, available at http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm

[15] See Convention 108, art. 8 a)

[16] See Principle VII d) of the OECD Privacy Principles, Principle II of the UN Data Protection Principles & Rights, and art. 8 d) of Convention 108.

[17] See Convention 108, art. 8 c)

[18] This is a corollary of the right to one's own identity, which forms integral part of the right to privacy

[19] See Opinion 15/2011 of the Article 29 Working Party on the definition of consent, p.33

[20] See article 8 b) of Convention 108

[21] See article 8 f) of Convention 108, and Part IV of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

[22] See Article 29 WP Opinion (WP225/14) on the implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez", C-131/12; available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

[23] This is, once again, in respect of the individual's right to identity, see supra note 15. The exception for public interest purposes is intrinsic to the notion of right to informational self-determination. In part, it refers to the notion of "public figures" which was specified in Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the Right to Privacy; it is also specifically addressed through the relevant human rights jurisprudence (see e.g. Von Hannover v. Germany (no.2), 2012) and most recently, through the Art. 29 Working Party's Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González " C- 131/12

[24] *Ibidem*

[25] See Guiding Principles, Part II, section B, para. 21. The Google transparency report is a role model in this field. See http://www.google.com/transparencyreport/

[26] In Sweden, for example, journalistic products such as newspapers, even if privately owned, abide by specially designed laws that grant them a special legal status because of their potential for free speech.

[27] See Council of Europe, Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media, para. 6

[28] *Ibidem*

[29] On that regard, the Johannesburg Principles on National Security, Freedom of Expression and Access to Information provide further guidance on how and when restrictions to freedom of expression may be exercised.

[30] See Manila Principles on Intermediary Liability, 3.b; available at https://www.manilaprinciples.org/

[31] See the Global Network Initiative Principles on Freedom of Expression and Privacy; available at https://globalnetworkinitiative.org/principles/index.php

[32] See for instance, those provided by CommonTerms (see www.Commonterms.org) and Aza Raskin (see http://www.azarask.in/blog/post/privacy-icons/)

[33]Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum, para. 90

[34] Council of Europe Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum, para. 95

[35] See Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet. Decl-20.02.2008/2E

[36] See Council of Europe Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, para. II.8

[37] See EU Directive 95/46/EC, Article 2(h)

[38] See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27

[39] See e.g. Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms

[40] See Council of Europe, Committee of Ministers" Recommendation 97(20) on "hate speech"

[41] In the case of restriction to freedom of expression, the legitimate purpose shall be one of those set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals. While no specific legitimate objectives have been identified by the Special Rapporteur to evaluate restrictions to privacy, the test devised in the Report is roughly equivalent, requiring that measures encroaching upon privacy be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others. See 2011 Report, para. 59

See Explanatory Report of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), para. 28

[42] See e.g. Council of Europe, Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum

[43] See the Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, according to which "a person is identifiable if, on the basis of any means likely reasonably to be used either by the data controller or by any other person, he or she can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

[44] See U.S. National Institute of Standards and Technology (NIST), NIST's Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), available at: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf. See also the Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, according to which "a person is identifiable if, on the basis of any means likely reasonably to be used either by the data controller or by any other person, he or she can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

[45] In the case of restriction to freedom of expression, the legitimate purpose shall be one of those set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals. While no specific legitimate objectives have been identified by the Special Rapporteur to evaluate restrictions to privacy, the test devised in the Report is roughly equivalent, requiring that measures encroaching upon privacy be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others. See 2011 Report, para. 59