The right to privacy in the digital age

UNESCO's inputs for the preparation of the thematic report of the Office of the United Nations High Commissioner for Human Rights

UNESCO's inputs have specifically addressed the issues hereby listed:

- targeted and mass surveillance, including of journalists and human rights defenders;
- use of publicly accessible information and data by state authorities, for example when monitoring social media;
- tracking of internet users;

I. Trends and challenges with regard to the promotion and protection of the right to privacy in the digital age

Freedom of expression and the right to privacy are among the human rights most impacted by the digital transformation. Interrelations between these rights have too been transformed. In the pre-Internet world, freedom of expression and privacy were thought to be contradictory, and only interacting when journalists reported on public figures in the name of the right to know, or when the privacy of a journalist was invaded.

With the advent of the digital age, the right to privacy and freedom of expression have become interdependent, as is for example demonstrated by the chilling effect that privacy violations can have on media freedom: monitoring of online activity, data retention and big data, Artificial Intelligence-powered territorial surveillance and hacking are all developments who simultaneously threaten our individual privacy and the free exercise of journalism.

The latest UNESCO World Trends Report Insights discussion paper "Threats that Silence: Trends in the Safety of Journalists" highlights how surveillance and hacking are compromising journalism. This was vividly shown in exposés by investigative journalists and researchers, giving rise to UN human rights experts calling for a temporary global moratorium on the sale and transfer of surveillance technology.

The growing sophistication and undetectability of mal- and spyware and their increasing use against journalists and human rights defenders by state and non-state actors, endanger free and independent journalism. Surveillance can expose information gathered by journalists including from whistle-blowers, and violates the principle of source protection, which is universally considered a prerequisite for freedom of the media and is enshrined in UN Resolutions. Privacy is a pre-requisite for journalists to do their work and ensuring our access to fact-based and reliable information. It is a necessity if they are to communicate freely with sources, receive confidential information, investigate corruption, and guarantee the safety of themselves and their sources. Surveillance may also harm the safety of journalists by disclosing sensitive

private information which could be used to reprisals such as threats, harassment, arbitrary detention, torture, and killings.

These technologies are increasingly easy to obtain, due to the lack of strong legal safeguards, as most legislation on surveillance fails to keep up with technological innovations. Under the guise of security, journalists and other legitimate actors are targeted, while national oversight of security operations and security laws are inadequate. This also imperils our collective right to access to information and privacy.

In addition, the COVID-19 pandemic has driven home just how powerful the internet economy has become. Social, political and economic life has significantly moved online, and many aspects of societies are now dependent upon internet companies. As the public and societal importance of internet companies becomes more apparent, questions about how an ecosystem, upon which we all depend, is made democratically accountable have become more urgent.

Increased reliance on digital services means that citizens often unknowingly share private information and data in exchange for free services. Individuals' data leaves behind a "digital footprint" that can be analysed in real time or ex-post by hostile and illegitimate actors. Moreover, data held by Internet and cybersurveillance companies about personal lives can often be obtained by authorities without adequate due process or transparency.

New technologies are increasingly key to define the ways citizens relate to information, and often put forward situations where the balance between rights such as privacy and freedom of expression need to be carefully examined by judicial actors. Technology, indeed, contributes to add more complexity to this context. Informational rights, such as privacy, access to information, freedom of expression and others, should today be considered by their intrinsic value but also as instrumental rights, as they enable several other rights and liberties that increasingly depend on information and communication technologies to be fulfilled. In such a scenario, privacy and data protection, other than opposed, should be considered as complementary to freedom of speech.

In light of the above, there is a growing global push encouraging more transparency regarding how Internet companies exploit citizens' data, how it informs predictive models and artificial intelligence, and enables amplification of disinformation and hatred. This was underlined in the Windhoek+30 Declaration call for technology companies to "work to ensure transparency in relation to their human and automated systems". Improved transparency by internet companies would make them more accountable for their operations and provide more information regarding the impact on increasing areas of social life.1

II. Related human rights principles, safeguards and best practices

a) Legal principles to balance the right to privacy and other fundamental rights, including freedom of expression

New and innovative data-intensive technologies increasingly make up the interface between the individual and other entities – other individuals, governments, employers, companies - increasing risks to

[1] UNESCO Issue brief: Letting the sun shine in: transparency and accountability in the digital age

data protection and privacy, as well as freedom of expression and other rights, as various areas of human activity are mediated by data.

In this context, UNESCO has developed the Guidelines for judicial actors on privacy and data protection which aim to provide a general framework for judicial actors to assess matters of privacy and data protection in the face of other rights, such as freedom of expression and the right to privacy.

The right to private life is recognized by various international human rights instruments, such as among others the 1948 Universal Declaration of Human Rights (art. 12), the 1966 International Covenant on Civil and Political Rights (art. 17), the European Convention on Human Rights (art. 8), the African Charter on Human and Peoples' Rights and the Arab Charter on Human Rights (art. 16, 8). The concepts of privacy and private life are frequently used interchangeably.

When the right to privacy and other human rights are at odds, the ***proportionality principle*** is the main legal tool used to balance the different human rights. Then, a balancing test needs to be made, which is based on the principle of proportionality. This usually concerns interferences of the State into the rights of individuals, thus frequently translating into an opposition between collective and individual interests. The proportionality test is explicitly applied in the context of the European legal systems (ECJ and ECHR), the African regional legal framework (ACHPR), the East African Court of Justice (EACJ), and the American regional human right system (IACHR) and has been gaining space in various decisions of the Human Rights Committee (HRC).

The proportionality test revolves around three steps: suitability (whether the interference is actually suited to achieve the alleged aim), necessity (also "less restrictive alternative" or "minimal impairment"; whether the measure taken is the least restrictive alternative) and proportionality in the strict sense (whether the benefits achieved are outweighed by the limitations caused). It is also usually preceded by two additional tests of legality (whether the interference is based on national law) and legitimate aim (whether the interference pursues one of the aims dictated by the limitation clauses present, respectively, in the Covenant on Civil and Political Rights (ICCPR), ECHR, ACHPR or ACHPR).

The Regional Human Rights Courts follow the 3-part test to establish a violation of the privacy rights afforded in the relevant Conventions. These are based on the concepts of lawfulness, legitimacy and necessity in a democratic society.

1. ***Lawfulness*** refers to the existence of a previous and accessible law, enacted through a valid process that authorizes the actions of the particular person or authority. In other words, the interference needs to be based on domestic law that is accessible (Shimovolos v. Russia), foreseeable (Rotaru v. Romania) and accompanied by effective "safeguards [against abuse] established by law".
2. ***Legitimacy*** refers to the ends of the action— if they pursue a legitimate function regarding the Conventions, namely: national security; public safety; the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals; or for the protection of the rights and freedoms of others.
3. ***Necessity*** is characterised in the absence of a less restrictive alternative and, in this case, also resonates with elements of strict proportionality as it compares the potential impact of the action on rights to the potential benefit derived from it.

It is important to highlight that the move from a diminutive conceptualization of privacy as the right to be let alone to an expanded sphere of private life rooted in the realization of human dignity brings about a change to an increasing volume of positive obligations of the State, where more structures and institutions may be needed. In other words, there is an actual need for the state to put in place the necessary structures and institutions for the protection of rights. This will be expanded upon and made even clearer when we touch upon data protection rights, which involve many such obligations, from providing access to information to ensuring due process, guaranteeing control over personal data and stopping unauthorized disclosure of personal data etc (Gaskin v. the United Kingdom). The evolution of data protection legislation is nearly a fact of the development of information and communication technologies and its effects on how people's information is used.

There is a selection of principles, concepts and rights that should be taken into account when measuring the balance of decisions of privacy and data protection rights in the face of other fundamental rights. The principles generally recognized as the basis for data protection regulations are:

- ***Purpose limitation***: data processing activities should be tied to a specific purpose which is made known to the data subject beforehand.
- ***Minimization or necessity***: no more data than that which is strictly necessary to realize this purpose should be processed.
- ***Transparency***: a data subject must have knowledge and understanding of the collection and treatment of their data.
- ***Quality or accuracy***: data on a subject should be precise and updated.
- ***Access***: the data subject should be able to access their data.
- ***Security***: data controllers should apply appropriate technical and organizational security.

It is important to stress that public figures, particularly politicians, people with incidence in public life or in a position of responsibility, still hold their privacy rights; however, some consideration must be given to the fact that they can attract attention and their position may limit in some cases their expectancy of privacy. Particularly relevant is the fact that some of their acts, as they may be subjected to public scrutiny, mustn't be covered by privacy rights or other means.

Conclusions and recommendations to balance the right to privacy and other human rights and fundamental freedoms:

1) The right to data protection is recent compared to freedom of expression rights and, as such, any evaluation about it should consider its presence in ongoing trials, debates and documents and also its instrumental nature as an enabler of other related human rights, besides its gradual yet constant evolving presence in human rights documents and statutes.

2) As information and communication technologies intensify the availability of information and its uses, the right to data protection and freedom of expression must more and more be mutually evaluated and considered. In this sense, cases which would be typically analysed according to freedom of expression standards may also increasingly demand the consideration of the data protection rights potentially (or actually) involved —and vice-versa.

3) The three-part test is an adequate and viable instrument to consider the interactions between data protection and freedom of expression rights and should be employed in order to keep them both substantial at their maximum extent.

4) The right to data protection and freedom of expression both evolved from technological innovation. Thus, the balancing of such rights should consider both the technological impact to them —in terms of risks and harms— as its eventual impact to the use of these technologies, as the very possibility of exercising these rights is often provided by technologic features themselves.

b) Principles and good practices for more transparency of internet companies

Transparency has become a buzzword in the field of digital technology, fueled by the increasing dominance of internet companies in public life and, alongside their benefits, also their potential for causing harm to human rights. Transparency, drawing from the use of the term in relation to the universal right to freedom of information, has a dual dimension. It covers arrangements for access to information and data, as well as those for proactive disclosure.

Such arrangements make it possible for external stakeholders to gain insight into the impact of companies upon people's ability to express themselves, protect their privacy, access journalism, recognise and counter hate speech and disinformation, and share and exchange knowledge.

In many countries, a degree of transparency is required by law around ownership and the legal status of corporate actors, although controls may still sometimes be hidden. In other cases, companies must provide transparency about their handling of content. Beyond legal requirements for transparency, a growing number of companies have committed to self-regulatory actions, jointly or individually, such as in publishing voluntary transparency reports. Such reports (around 70 by 2018, according to Access Now) contain information such as the number of governmental requests received and responded to over a particular time period.

Beyond the actions of governments, private internet companies are facing increased scrutiny into how they deal with speech that is not protected under freedom of expression standards, and how they use personal data to impact what users see in their search results, content feeds, and recommendations. As part of growing multi-stakeholder support for enhanced transparency as a means of increasing accountability, UNESCO has developed a brief on Transparency and Accountability in Digital Age where a selection of 26 high-level principles that can serve as a guide to companies, policymakers, and regulators are set out.

These illustrative high-level principles could apply broadly to those internet companies which provide services around finding, creating, discovering, sharing, curating, prioritising, monetising, communicating and editing content.

General:

1. Companies should explicitly recognise they have an obligation to protect human rights, and particularly freedom of expression and access to information, and the privacy of their users;

2. Companies should recognise the need for the proactive disclosure of information as well as responding to requests for information;

3. Companies should be transparent about ownership and control, including of their subsidiary company(ies);

4. Companies should indicate what kinds of commercially-sensitive data they do not wish to disclose.

Content and process transparency:

5. Companies should be transparent about any terms and standards they enforce on their own platforms, setting out the limits of what they deem to be acceptable behaviour, and how these parameters align to respect for international standards for freedom of expression;

6. Companies should be transparent about any processes they have in place to identify, remove or reduce the impact of disinformation and hate speech, including pre- and post-publication measures; and how such processes respect the free exchange of ideas and opinions;

7. Companies should disclose what percentage of content is automatically and pro-actively removed compared to the percentage that is removed as a result of complaints;

8. Companies should be transparent about any processes they have in place to identify and act against inauthentic behaviour and false identities when these are used to undermine human rights;

9. Companies should disclose whether their processes for removing content and prohibiting behaviour are periodically subject to third party assessment as to human rights compliance, carried out by a respected external independent institution or oversight body; and consider whether such assessments should themselves be transparent as well as the company's own response to any recommendations arising.

Due diligence and redress:

10. Companies should be transparent as to whether they have processes to enable people to raise concerns about content, including that which appears to violate human rights or advocates incitement to violence, hostility or discrimination, as well as inaccurate content; and they should be transparent about implementation of such processes in terms of numbers and types of complaints and actions taken;

11. Companies should be transparent about whether they conduct risk assessments for their operations, such as in contexts of upcoming elections or in countries in conflict, highlighting any serious potential threats to freedom of expression, privacy and other human rights, as well as their proposals for mitigating those threats;

12. Companies should disclose if they have risk assessments of any algorithms whose application can have the potential to discriminate against people unfairly, and if there are any proposed mitigation measures;

13. Companies should publish guidelines for how they will develop ethical AI processes which make consequential decisions that can impact on human rights.

Empowerment:

14. Companies should disclose any efforts they make which help to promote the media and information literacy competencies of those who are using their services;

15. Companies should disclose the terms and conditions for grants made in support of research, education and advocacy, as well as lobbying activities.

Transparency and commercial dimensions:

16. Companies should provide information about political advertisements, including the author and those paying for the ads, and should retain these advertisements in a publicly accessible library online;

17. Companies should reveal practices of advertising and data collection regarding children's rights;

18. Companies should enable individuals to find out on what basis they are being targeted for advertising.

Personal data gathering and use:

19. Companies should provide information that enables people to have a meaningful (i.e. concise, transparent, intelligible, reasonably comprehensive and easily accessible) understanding about what kinds of personal data are collected and how these are used;

20. Companies should provide the means for the user to check the accuracy of their personal data held by the service, and disclose how people can request amendments or deletion in line with privacy and data protection principles;

21. Companies should state how many government requests for access to personal data have been received and the legal status of those requests;

22. Companies should disclose if and how their processes for managing privacy and data protection are subject to third party assessment by a respected external independent institution (or oversight body), following an agreed standard that respects human rights;

23. Companies should disclose their use of tracking cookies, or other systems, that gather user data on their and other services across the internet, and with whom they share this data;

24. Companies should disclose data breaches and what actions are being taken to strengthen data security.

Data access:

25. Companies should, in an analogous fashion to many public statistical bodies, have a process to allow researchers access to personal data they hold, where this will advance important public interest goals such as open access and open science, while guaranteeing users' privacy through the range of necessary measures;

26. Companies should be transparent about their third-party agreements which allow access to personal data that is purchased, shared, directly harvested or held by them.

Conclusions and recommendations for more transparency of internet companies

1. While transparency proposals are usually presented as part of a general approach to making internet companies more accountable, embracing transparency is also in the companies' own self-interest. Enhanced and systematic transparency can help correct the problems and bring more of the benefits to light. In addition, transparency reporting allows companies to demonstrate their fulfilment of corporate social responsibility, over and above what is required by law. In this sense, the application of a set of global principles for transparency by a company could be a competitive advantage, as well as provide for more consistent standards internationally.

2. These illustrative high-level principles should be discussed as a first step in developing a more detailed approach to transparency:

- ***Companies*** should discuss these principles and commit to develop them further into a framework for transparency across the platform industry.
- **Regulators** should reflect on these principles as the basis for incorporating transparency provisions in future regulatory initiatives, and as a benefit for developing evidence-based policies related to the internet and AI. Appropriate regulators could also engage in collaborative dialogue with other regulators that deal with internet companies (such as competition, data protection and privacy), to provide agreed and consistent expectations of transparency.
- ***Governments***, in considering whether or how to regulate internet companies, should examine how transparency principles can contribute to achieving public policy objectives in place of more intrusive legislation that can pose risks to freedom of expression.
- **Civil society** should encourage elaborated transparency objectives in their advocacy for greater accountability among internet companies and raise these issues with national regulators and policy makers.
- ***Academia and the technical community*** should give more attention to the issue of transparency in their research priorities as well as in further development of the internet architecture.