The European Union Institutions would like to thank the Secretariat of the Human Rights Council Advisory Committee (Office of the High Commissioner for Human Rights), for its call for contributions on new technologies and human rights. As recommended in the Note Verbale, your questionnaire was used to facilitate the input provided.

The structure of the reply is twofold. The first part (I) focuses on answering the "core questions for all stakeholders", while the second part (II) provides a state of play of the current EU policies and initiatives on human rights and technologies. Some of the EU policies briefly mentioned in (I) are detailed further in (II).

I. Core questions (for all stakeholders)

1. In what ways do new and emerging digital technologies help to protect and promote human rights? How can the positive benefits of these technologies be realized?

It is widely acknowledged by governments, UN experts, Civil Society Organisations (CSOs) and academia that new technologies can have a positive impact for the protection and promotion of human rights.

CSOs and human rights defenders can for instance easily document human rights violations thanks to new technologies, as well as storing and exchanging information safely through encrypted communication channels. Shrinking space for civil society can be countered by enabling accessible digital environments, including by fostering open internet. Government, international organisations, human rights researchers can also make use of satellite images to document human rights violations that otherwise would be hard to witness (e.g.: secluded detention camps, flows of forced displacement).

New technologies such as facial recognition have allowed the reunification of refugees with their families, while the spreading of databases has enhanced the possibilities to identify victims of enforced disappearances.

Furthermore, the development and new tech applications and Artificial Intelligence (AI) can increase access to education and health care services around the world, including in remote areas and for vulnerable groups (elderly, persons with disabilities).

Finally, emerging technologies can offer persons with disabilities greater inclusion and participation in society in line with the UN Convention on the Rights of Persons with disabilities. This Convention identifies Information and Communication technologies (ICT) as an enabler that can help address longstanding barriers of communication, interaction and access to information for persons with disabilities.

The potential of new technologies and AI to promote human rights still has to be explored. Governments and CSOs need more training on how to use these new tools. It is important to ensure that CSOs and human rights defenders (HRDs) have safe ways of communicating and documenting their work.

2. What are some of the key human rights challenges arising from new and emerging digital technologies? How can these risks be mitigated? Do new and emerging digital technologies create unique and unprecedented challenges or are there earlier precedents that help us understand the issue area?

The risks of new technologies for the promotion and protection of human rights are equally acknowledged.

Without being exhaustive, we can think of some major challenges. We are witnessing how hate speech and fake news are spreading at an alarming speed in the digital sphere including through social media platforms. Hate speech is often an early warning sign of persecution, and has triggered hate crimes against individuals because of their gender, religion, or ethnic origin. Disinformation campaigns, often structured by the

development of algorithms and bots, are known to have influenced electoral processes as well as to have fostered campaigns of hate against minorities.

New technologies are also being widely used by some government to carry out mass and arbitrary surveillance of their citizens, which allow them to crack down easily on civil society movements and dissent. Regular breaches to privacy are another common trend that we can observe.

The development of AI also presents risks. For instance, the use of predictive algorithms in law enforcement (work of security forces and the judiciary, in particular predictive policing) can lead to reinforce discriminations and biases, by over-targeting minorities. We can observe a similar phenomenon when AI is used for scrutinising job applications, or for credit-scoring purposes.

A group that can be particularly vulnerable to technology are children. While child sexual abuse is not a new phenomenon, the scale, speed and ease of access to such illegal online material is unprecedented. Pre-existing risks, such as cyberbullying and exposure to harmful content, have also changed tu to the increased capacitcy to constantly remain online, in contact with others.

Even if it is more a matter of international humanitarian law (IHL), new technologies have increased the development of autonomous weapons, which can escape human control and agency.

We also have to consider that accessibility to new technology and digital literacy is not equal. Vulnerable groups (persons with disabilities, people working in remote and rural areas, persons with low economic resources) might have less access to new technologies, which reinforces existing barriers. It is needed to promote the accessibility of technologies and of an open internet for all, paying a special attention to access for vulnerable groups, including persons with disabilities, since the early stage of design of new technologies. It should be ensured that the whole of society can benefit of the tremendous potential of digital opportunities, in terms of education, employability, and participation in social and political life.

Some of the challenges that we are facing now are not necessarily new (discrimination, limitations on freedom of expression, illegal surveillance, hate speech), however through technologies, they can spread at a faster space and in a wider scale. Technology by facilitating anonymity also makes it harder to identify the author of human rights violations. It is possible to build up on past experiences to try to address the challenges of nowadays, bearing in mind the inherent transnational character of new technologies. In addition, the development of AI, is still at the moment a rather uncertain territory when we try to evaluate its impact on human rights. Further monitoring and development of expertise is necessary.

Possible solutions are explored in the upcoming answers, such as the need to work with the private sector, to enhance multilateralism and sharing of experiences. In the second part of our reply, our current policies to prevent human rights violations are detailed, in particular regarding data protection, hate speech, rights of the child, AI, empowering CSOs. We believe that EU's experience can be valuable to other actors in the UN fora.

3. Is the existing international human rights framework adequate to safeguard human rights in an era of rapid technological innovation? Why or why not? If not, what types of reforms are needed?

As mentioned in the previous answer, some of the human rights breaches caused be new technologies are not new (discrimination, limitations on freedom of expression etc.), hence the the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights, remain fully valid texts that guide our work.

The Declaration, Covenants, and relevant UN Conventions, are being dully complemented by resolutions in the Human Rights Council (HRC) and UN General Assembly Third Committee, that have proven adaptable to changing external events and that provide adequate guidance to the international community (e.g.

resolutions on the enjoyment of human rights on the internet; on the rights to privacy in the digital age). We also welcome the guidance on the matter of several UN Special Procedures, such as recommendations of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

Internationally, we understand that while the current human framework is relevant, discussions are emerging on its possible adaptations, at HRC and UN General Assembly 3rd Committee. We fully support the on-going efforts led by the OHCHR to stir a reflexion on new technologies and human rights, and we hope that that your upcoming report (2020) and panel of experts (2019) at the HRC will provide leads on whether the international human rights framework should be adapted or not. The human rights framework has to be agile, realistic and flexible enough to effectively redress context-specific issues and contradictions that new technologies present us with.

We echo the call made in the report of the UN Secretary-General's High-level Panel on Digital Cooperation of the "*urgent need to examine how time-honoured human rights frameworks and conventions – and the obligations that flow from those commitments – can guide actions and policies relating to digital cooperation and digital technology*"

We also agree with HRC resolution 41/11 that states: mindful of: "*impacts, opportunities and challenges of rapid technological change with regard to the promotion, protection and enjoyment of human rights, including in cases where changes may occur at an exponential pace, are not fully understood, and of the need to further analyse them in a holistic, inclusive and comprehensive manner"*

To note, that within the EU, since the entry into force of the Lisbon Treaty in 2009, the EU institutions must guarantee that the rights and principles of the charter are correctly taken into account at every step of the legislative process, including in relation to regulatory acts and policies in the digital field. Since all proposals for EU legislation must respect the Charter, the Commission has ensured a system of assessing the impact on fundamental rights as an important feature of the impact assessment.

To mitigate the impact of technology on human rights, the EU for instance has developed new legislation to uphold data protection and in the upcoming months will issue new legislation on AI (see: II. State of Play of EU policies).

4. In your opinion, are there any gaps or overlaps in existing efforts to respond to the issue of new and emerging digital technologies? Are some human rights or technologies being overlooked?

It could seem that actions in response to the impact of new technologies focus mostly on freedom of expression online, hate speech online or disinformation, while privacy and data protection is also increasingly addressed (in particular within the EU, with the new regulation on data protection).

Our diplomatic experience shows us that the use of new technologies for mass-surveillance purposes is less addressed. It might be due to a lack of knowledge of the international community or perhaps to a lack of willingness of certain actors, in particular when national security concerns are driving their political agenda.

Technical expertise on AI's impact on human rights is currently being developed as it is still a rather unknown field. We believe that the consequence use of AI technologies and algorithms by States to deliver public services should be further explored. The EU believes that it is essential to uphold some key principles such as human agency and oversight, and non-discrimination. We believe that vulnerable users from diverse backgrounds (children, persons with disabilities) need to be involved in the development of AI, in order to ensure that AI is non-discriminatory and inclusive.

Overlaps might exist as several international organisations and UN member states are developing policies on this field. This is the case for the EU, the UN, the Council of Europe; discussions have also emerged during international summits such as the G20.

Thanks to your worldwide consultation, initiatives from all over the world will be mapped, allowing to identify overlaps and potential burden-sharing as well as possible gaps.

5. As opposed to focusing on a selected few technologies, do you think a holistic and inclusive approach will help reduce any gaps in the existing system for addressing human rights challenges from new and emerging digital technology?

The EU favours a general analysis and a comprehensive approach to tackle all challenges presented by new technologies to human rights.

Only a comprehensive approach to the human rights challenge is desirable, granted the fast changing nature of technological developments. Yesterday's focus on jurisdiction or copyright has been quickly replaced with today's issues of hate speech online and AI, only to make potentially way for tomorrow's new challenges.

The global consultation that you are driving will hopefully allow you to identify which stakeholders are leading efforts in mitigating different impacts of new technologies. Once identified, it would be important to share conclusions and recommendations and organize multilateral discussions where best practices can be shared, in order to shape comprehensive policies.

The upcoming debates require consideration of two elements: the multi-stakeholder nature of technological and internet governance; and the global, transboundary character of cyberspace, necessitating effective international dialogue between and among all involved stakeholders. Only through effective dialogue with key stakeholders: business (including the technical community) and civil society (including academia) we can build an effective approach to tackling the global challenge of enforce human rights compliance of new technologies.

6. What should be the role of the private sector in mitigating the risks of new and emerging digital technologies to human rights? What about the roles of other key stakeholders?

Most technological innovations are being developed by the private sector, whether it is internet service providers and telecommunication firms, tech companies or social media platforms. Hence the need to involve them in the discussions seems absolutely necessary (not only on human rights aspects, but on all digital matters).

Joint identification of challenges, shortcomings, and solutions should be pursued. Private sector plays a crucial role in any co-regulation and self-regulation efforts. The EU has combined both logics, in certain occasion seeking to agree on self-regulatory practices (against hate speech online with social media platforms) or by regulating the online sphere (new data protection regime). We stand ready to share our experience on the matter. EU leaders have been increasingly discussing human rights compliance with representative of social media and tech companies. To note that an EU member state (Denmark) has appointed the first ever Tech Ambassador, who inter alia works on human rights.

Discussions should build on existing frameworks, such as the UN Guiding Principles on Business and Human Rights. We note with particular interest, the declaration of Michelle Bachelet, UN High Commissioner for Human Rights which in her opening statement of HRC 41st session (June 2019) declared: "*In the coming months my Office will be engaging with many voices across sectors and geographies to develop focused guidance on the application of the UN Guiding Principles on Business and Human Rights to digital technologies*".

In case of human rights violations, even if the State is the primary duty bearer, companies should avoid causing adverse human rights impacts and should seek to prevent or mitigate them. The systematization to the private sector of human rights impact assessment is key in this endeavour. The European Commission worked with think tanks to produce an "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights". The guide provides guidance to companies on setting out their commitment to respect human rights, to identifying and addressing their human rights risks, to providing remedy where actual harms occur.

If involvement and the responsibility of the private sector are important, States remain the essential duty bearers and have the obligation to take all appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication

As mentioned above, to draw a clear picture of the challenges and find comprehensive solutions a multi-stakeholder approach is needed. Independent civil society organization and human rights defenders have a unique role in documenting and monitoring negative impacts of new technologies, including in remote areas far from the international spotlight. They have a decisive role in tailoring recommendations towards states and international organisations. Accordingly, the EU pursues worldwide a policy to promote and protect CSOs and human rights defenders.

While independent media has an important role as well in documenting human rights violations, academia can conduct deep analysis of the impact of new technologies on human rights. EU representatives have liaised with human rights clinics on the matter (e.g. Human Rights Clinic of the University of Essex).

II- State of Play of EU policies on new technologies and Human Rights

Please describe the relevant work that your organization has done on the issue of new and emerging digital technologies and human rights. What have been the key accomplishments?

Besides answering conceptual questions, we consider important, through this contribution to provide a picture of the state of play of EU policies, projects and initiatives on human rights and technology. Over the last years the EU has developed tools to uphold high data privacy standards, combat hate speech online, protect the rights of the child, and ensure a human-centric approach to Artificial Intelligence.

Combatting hate speech online

The Commission has adopted initiatives to strike a balance between the need to ensure a safe online environment and the need to protect fundamental rights online. Namely the Code of Conduct on countering illegal hate speech of 2016, the Recommendation on measures to effectively tackle illegal content online of 1 March 2018, and the Proposal for a regulation on preventing the dissemination of terrorist content online of 12 September 2018.

To prevent and counter the spread of illegal hate speech online, in May 2016, the Commission agreed with Facebook, Microsoft, Twitter and YouTube a "Code of conduct on countering illegal hate speech online. In the course of 2018, Instagram, Google+, Snapchat and Dailymotion joined the Code of Conduct. Jeuxvideo.com joined in January 2019. On average, IT companies are now assessing 89% of flagged content within 24 hours, up from 81% one year ago. Removal rate remains stable at around 70%, which is satisfactory as hate speech is not easy to define. Its illegality has to be balanced with the right to freedom of expression and the context. The IT companies reported a considerable extension of their network of 'trusted flaggers' in Europe and are engaging on a regular basis with them to increase understanding of national specificities of hate speech. In the first year after the signature of the Code of conduct, Facebook reported to have taken 66 EU NGOs on board as trusted flaggers; and Twitter 40 NGOs in 21 EU countries.

For more information on the EU Code of Conduct, how it performs and its monitoring rounds, click here.

Data Protection

The EU has firmly increased safeguards for Data protection over the last years, in particular since 2018 and the entry into application of the General Data Protection Regulation.

Thanks to the General Data Protection Regulation (GDPR), there is one set of data protection rules for all companies operating in the EU, wherever they are based. Stronger rules on data protection mean people have more control over their personal data. The regulation is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. A single law will also do away with the current fragmentation in different national systems and unnecessary administrative burdens. A recent evaluation in May 2019 has shown that 67% of EU citizens are aware of the GDPR and highlighted that in its first year of existence, more than 144.000 queries and complaints have been received by all data protection authorities in Europe. Breaches of privacy have triggered legislative consequences such as fines for social network operators that failed to secure users data or for businesses that used unlawful video surveillance.

On data protection, two further pieces of legislation should be mentioned: the data Protection Law Enforcement Directive that protects the fundamental rights of victims, witnesses, and suspects of crimes,

whenever personal data is used by criminal law authorities for law enforcement purposes; as well as the Regulation on data protection by EU institutions and bodies that sets forth the rules applicable to the processing of personal data by European Union institutions, bodies, offices and agencies.

For additional information on date protection, in particular the GDPR: click here

Capacity strengthening of Civil Society Organisations (CSOs)

As highlighted earlier in our contribution, technologies can facilitate the task for CSOs and human rights defenders, for instance allowing them to articulate online effective advocacy campaigns, to document human rights violations or to access funds. However risks of surveillance and harassment exist. In order to take full advantage of the digital technologies, CSOs need more training on how to use these new tools.

EU external aid is supporting civil society organisations in working better with new technologies.

Through the European Instrument for Democracy and Human Rights (EIDHR) the EU has financed CSOs actions to increase protection of Human Rights defenders, including trainings on "cyber-hygiene" (practices and steps that users of computers and other devices take to maintain system health and improve online security.); train journalists for the digital age; or promote ethics in digital media.

The EU launched in 2018 an EIDHR Global Call of 5 million euros for CSOs which use new technologies to increase democratic participation. The selected projects will start in 2020. Some of the EU Delegations are also about to launch a call for proposals for CSOs on digitalisation and human rights (as well as direct budget support on digitalisation to governments).

One of our projects in a third country, for a value of one million euro, ensures that uses of bots in social media to promote disinformation are faced with transparency and media literacy practices. Through the uses of an algorithm that promotes transparency on bot behaviour in social media, the project aims to strengthen the ownership of CSOs (civil society organizations), news organizations and citizens in identifying and contextualizing disinformation campaigns. Outputs delivered by the project include content on bots and disinformation activity produced in partnership with news, fact-checking and civil society organizations

A "Supporting Democracy" project financed by the EIDHR has studied how CSOs can adapt to shrinking spaces by working with innovative solutions, including digital tools. The EU organised two regional conferences in 2019 in Kuala Lumpur and Beirut, which put together "traditional" CSOs and groups working on new technologies, to facilitate networking and cooperation.

To note that the Eastern Partnership Civil Society Facility organises regular "hackathons" to assist CSOs in developing new tools and participating in democratic life (example).

Protecting Children

We consider that digital technologies have become a powerful instrument for increasing access to education for children, but on the other hand, increasing use of digital technologies exposes children to various risks, violence and abuse. In a year that marks the 30th anniversary of the UN Convention on the Rights of Child, the EU has continued to safeguard children rights including in the online sphere.

The EU adopted a revised Audio-visual Media Services Directive to reinforce the protection of children when consuming audio-visual content. The Europol launched the #SayNO campaign already in 2017 to

provide children and adults with information on preventing and dealing with sexual extortion online. The initiative has been adopted in many EU countries and incorporated into education curricula in several.

In its Communications of 2016 and 2017 on online platforms, and on tackling illegal content online, the Commission stressed the need for online platforms to act more responsibly and step up EU-wide self-regulatory efforts to remove illegal content respectively. The 2018 Commission Recommendation on tackling illegal content online, proposes a common approach to swiftly and proactively detect, remove and prevent the reappearance of illegal content, including child sexual abuse material. The proposed measures concern: fast-track procedures for "trusted flaggers", new development of notification systems for users by technology companies, closer cooperation between authorities and technology platforms.

On a different note, this year, the EU-UNICEF global campaign for the 30th Anniversary of the CRC called #TheRealChallenge was launched. The aim of the campaign is to engage with children by creating space online for their participation.

Artificial intelligence

The European Union has been building an AI strategy and a coordinated plan to foster a human-centric approach to AI. Thanks in parts to the work of the High-Level Group on Artificial Intelligence (AI HLEG) , the European Commission launched the Communication on Building Trust in Human-Centric Artificial Intelligence in April 2019. Ensuring that European values are at the heart of creating the right environment of trust for the successful development and use of AI the Commission highlights the key requirements for trustworthy AI in the communication:

- Human agency and oversight
- Technical robustness and safety
- Privacy and Data Governance
- Transparency
- Diversity, non-discrimination and fairness
- Societal and environmental well-being
- Accountability

Aiming to operationalise these requirements, the Guidelines present an assessment list that offers guidance on each requirement's practical implementation and that is currently being tested. The political guidelines announced legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence.

In this Communication, and given the international interlinkages of AI development, the EU affirms its wish to: "*bring the Union's approach to the global stage and build a consensus on a human-centric AI"*, including" *by engaging in dialogues with non-EU countries and organising bilateral and multilateral meetings to build a consensus on human-centric AI"*. The development of AI research excellence centres is foreseen.

The new Commission president elect, Ursula von der Leyen has published her political guidance indicating that she will put forward a legal framework for a coordinated European approach on the human and ethical implications of AI within 100 days of the start of her mandate.

Developing Human Rights Expertise

The European Union Agency for Fundamental Rights (FRA) has been increasing its research on the field of new technologies and human rights. The FRA is the EU's centre of fundamental rights expertise. It is one of the EU's decentralised agencies who provide expert advice to the institutions of the EU and the Member States on a range of issues.

A couple of relatively recent research papers focus on artificial intelligence and big data:

- On data quality and artificial intelligence https://fra.europa.eu/en/publication/2019/artificial-intelligence-data-quality

- On big data and discrimination in data-supported decision making: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf

The FRA is also currently working on a research paper on facial recognition (to be issued towards the end of October 2019).

Technologies and Democracy

Technologies have also an impact on democracy. Even if it goes beyond the human rights framework, it is worth to highlight the EU vision.

The credibility of an election has always depended on the trust stakeholders have in the election management bodies (EMBs) and its management and administration of the process. The introduction of information and communication technologies (ICT) in areas such as voter registration, vote casting and results transmission, and the need to ensure these systems are cyber-secure, has added an additional set of challenges that can at times put these technologies at odds with the principles key to building trust in an electoral process: transparency, inclusiveness and accountability. As the introduction of the ICT may potentially affect these key principles, the confidentiality and accuracy of data in the election process should be preserved and protected. Therefore, consensual and cautious introduction of ICT should be considered in order to allow the building of public trust in ICT and at the same time work to avoid any potential conflict with the key principles for holding credible elections.

In the framework of the UN Declaration on Principles on International Electoral Observation, the EU is leading a concerted effort to draft guidelines for the observation of use of ICT in elections, together with work on defining the responsibility of different actors, including ICT producers and vendors, to ensure that the ICT complies with fundamental principles of transparency, inclusiveness and accountability.

Human Rights Diplomacy

The EU is increasing its human rights external action to address the consequences of new technologies on human rights.

We are increasingly raising our concerns with third countries for mass surveillance of citizens, internet shutdowns, and undue restrictions of freedom of expression online, while offering our technical expertise to combat illegal hate speech online and to foster internet access. We have channelled these discussions notably through our human rights dialogues (the EU has more than 40 dialogues each year with third countries and regional organisations).

Some of our upcoming work builds on the EU Human Rights guidelines on freedom of expression online and offline (adopted in 2014) which have among the priority areas of action the promotion and respect of human rights in cyberspace and other information communication technologies. Accordingly, the EU has repeatedly condemned restrictions to freedom of expression and access to the Internet, as well as the arrest of bloggers, in the framework of its bilateral relations with third countries and through several public statements.

It should be emphasized that the EU has also in the past, prohibited the export of technologies (equipment or software) to certain countries, in order to prevent authoritarian regimes to use them to crack down on human right defenders.

In line with our firm commitment to effective multilateralism we believe that the UN fora and in particular the Human Rights Council and UN General Assembly 3rd Committees are particularly relevant spaces to share best practices and recommendations while UN Special Procedures should provide expertise on the matter. We are fully committed to participate in the relevant upcoming discussions on human rights and new technologies in the multilateral fora.