Access Now Comments for the preparation of the future EU Action Plan on Human Rights and Democracy 2020-2024

April 2019

INTRODUCTION

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world.[1] By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age. We are a team of 60, with local staff in 12 locations across six continents.

Access Now welcomes the opportunity to provide input to the future EU Action Plan on Human Rights and Democracy 2020-2024. As we are unfortunately unable to attend the information session in person, we would like to take the opportunity to share our vision and proposals in writing. Our comments and suggestions focus on the protection and advancement of human rights in the digital era.

At home and outside its borders, the European Union has a responsibility to ensure that the digitalisation of society and the use of technology enables and respects not harms, human rights. The European Union has achieved important milestones to protect the digital rights of people living in the EU, notably by protecting net neutrality and by strengthening rules on the use of personal data. Through this type of user-centric regulations, which are so necessary in the digital era, the EU can leverage its diplomatic and economic power and influence, fulfilling its role to positively impact other regions and countries around the world.

While the 2015-2019 EU Action Plan included forward looking objectives such as the protection and promotion of freedom of expression online and offline, the document made no reference to digital rights or the digital economy, connectivity or the role of the internet in the promotion of human rights.[2] It is crucial that the next EU Action Plan on Human Rights and Democracy include a fully-fledged digital strategy to ensure that the EU's human rights agenda is adequate for the digital age and centred in protecting people's' human rights.

This process is an opportunity for the EU to reflect on the outputs of the past 15 years of its Digital Agenda and Digital Single Market strategies. It is important to identify the areas where the EU has missed the opportunity to reap the potential of digitalisation, and where it has failed to fulfill its duty to protect human rights.

[1] https://www.accessnow.org/
[2] https://eeas.europa.eu/sites/eeas/files/eu_action_plan_on_human_rights_and_democracy_en_2.pdf

In our substantive comments below, we make recommendations for the EU to become a leader in the protection and advancement of human rights in the digital era for users around the world, including in key areas such as connectivity, privacy, the rule of law and, artificial intelligence.

Lastly, we believe the EU should **stand up for the protection of human rights defenders, NGOs and civil society** in general. An independent civil society and an open civic space is necessary in all functioning democracies, in Europe and abroad. The formal and informal crackdown on civil society is no news in many regions, and it is thus pressing to find a solution to these increasingly problematic developments and realities.

The EU is seeing these challenges unravel within its own borders as a number of member states are conducting legal changes to limit human rights, the independence and powers of democratic and judicial institutions leading to the deterioration of civic space and curtailing freedoms. The EU must act as a bulwark to contain these developments.

Access to the internet is an enabler for human rights

Internet connectivity is essential for economic, social, cultural, political, and civic participation in the digital age. As expressed by the former United Nation Special Rapporteur on Freedom of Expression Frank La Rue, "the Internet is one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies."[3]

For the benefits of information and communications technologies to spread equitably and freely, connectivity must occur within a human rights framework. To that end, Access Now has developed the **Human Rights Principles for Connectivity and Development**.[4] These principles seek to achieve the Sustainable Development Goals (SDGs) using information and communications technologies and to prevent, mitigate, and remedy human rights harms that arise in development projects linked to internet infrastructure and connectivity.

Promoting connectivity requires **guaranteeing the openness of the internet and the principle of Net Neutrality**, according to which all internet traffic should be treated equally.[5] Net Neutrality is central to maintaining the internet's potential for economic and social development, and for the exercise of internationally recognised human rights such as the right to free expression. This principle helps ensure that anyone, anywhere in the world, can receive and impart information freely over the internet, no matter where they are, what services they use, or what device they operate. This principle is now protected in law in many jurisdictions around the world, including in the European Union through Regulation EU/2015/2120.

Despite the EU Regulation, the problematic so-called "zero rating" practice persists. With "zero rated" offers, the content of some apps or online services do not count against the amount of data

[3] https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[4] https://www.accessnow.org/cms/assets/uploads/2016/10/The-Human-Rights-Principles-for-Connectivity-and-Development.pdf

[5] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863

that is sold by the telecom operator. Other times, “zero rated” offers allow users to continue using certain apps or online services once the data limit is reached. Another typical model occurs when a telecom provider prioritises either its own content or data sponsored by third parties in the network, thus distorting competition and infringing on the right to receive and impart information.

While this may seem like an economic benefit for users, in practice, this amounts to a very problematic splintering of the internet as users get access to only some, but not all, of the internet. The most frequent model being “sub-internet” offers, where only few selected hand-picked websites are offered for “free”. All forms of zero rating amount to network discrimination and constitute a global threat to the open internet. **The EU should advocate for the ban of all forms of zero rating programmes towards its partners around the world**.

Finally, it is important to note that Regulation EU/2015/2120 only deals with residential connectivity or so-called *last mile*. This means that the Regulation does not impose any non-discrimination obligation on operators handling traffic beyond that point. In consequence, it is important for the EU itself, and with its global partners, to look carefully into any discriminatory and anticompetitive practices that may exist within transit and peering networks, content delivery networks, and more. **The principle of net neutrality should apply across all layers and levels of the global internet infrastructure.**

Another very problematic connectivity issue for human rights are **internet shutdowns**, which have increased in recent years. An internet shutdown happens when someone — usually a government — intentionally disrupts the internet or mobile apps to control what people say or do. Shutdowns are also sometimes called “blackouts” or “kill switches.”

Internet shutdowns violate human rights including both civil and political and economic, social and cultural rights. Internet and connectivity disruptions disproportionately impact vulnerable groups including human rights defenders. On top of human rights violations, internet shutdowns harm the economy. The Global Network Initiative and the Brookings Institute published reports that found that an average high-connectivity country stands to lose at least 1.9% of its daily GDP for each day all internet services are shut down.[6] The study concluded that internet shutdowns cost countries $2.4 billion in 2015. Despite these human rights and economic harms, the number of shutdowns is skyrocketing. In 2018, the #KeepitOn coalition, coordinated by Access Now, has tracked 188 Internet shutdowns, more than double than the number of cases reported in 2016.[7] Asia and Africa are the most affected regions where some shutdowns have lasted as long as 230 days.

Internet shutdowns often happen before and during elections, organised protests and visits by government officials. When a shutdown happens in these circumstances, it prevents important information such as voting or security notices from reaching citizens. It also prevents people from documenting human rights violations such as the disproportionate use of force by the police or military. Shutdowns impact democratic processes by preventing opposition candidates and parties to communicate with supporters or expose and document illegal activities. They further

[6] https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/
[7] https://www.accessnow.org/keepiton/

prevents journalists, election monitors, and ordinary citizens from reporting fraud or irregularities at polling places.

The EU has an important role in election monitoring around the world and should **join the fight against internet shutdowns**. More specifically, **the EU should**:

- Unequivocally condemn measures that are in violation of international human rights law that prevent or disrupt an individual's ability to seek, receive or impart information online,
- Advocate for increased attention to shutdowns at the United Nations, through Human Rights Council and General Assembly resolutions, including to monitor and communicate on the impacts of shutdowns on a range of human rights,
- Pledge greater financial and technical support to the UN and similar intergovernmental bodies to carry out monitoring and awareness-raising activities around shutdowns,
- Require European telecom service providers operating in countries where internet shutdowns are taking place to be transparent on shutdown orders given by governments,
- Call upon all States to refrain from and cease measures disrupting networks and ensure that all domestic laws, policies and practices are consistent with their international human rights obligations with regard to freedom of opinion and expression online,
- Ensure that all EU election observer missions include internet shutdowns in their election monitoring criteria and evaluation,
- Support organisations that do measurements to capture technical evidence and tracking of shutdowns, and finally
- Invest in supporting organisations that research and analyse the costs and impacts of shutdowns and provide support to affected communities.

The rights to privacy and data protection are an essential pillar to protect democratic processes

In the digital era, sharing data has often become necessary for us to do everyday tasks and engage with other people in today's society. This practice is not without risks as personal data reveals a lot about a person's life, habits, thoughts and communications. These data can be exploited for harmful purposes, and that is especially dangerous for vulnerable individuals and communities, such as journalists, activists, human rights defenders, and members of oppressed and marginalised groups.

In the European Union, data protection is a fundamental right recognised under Article 8 of the EU Charter, and further protected under Article 16 of the Treaty on the Functioning of the European Union, and the General Data Protection Regulation EU/2016/679 (GDPR). The EU also recognises a separate right to privacy protected under Article 7 of the Charter and through the ePrivacy legislation which is currently being reformed. Thanks to these measures, the EU is a leading actor on the global scene for the protection of personal data and the confidentiality of communications. But threats to these rights continue to multiply as a few but powerful private and public actors vigorously lobby to water down these norms and their enforcement. In the meantime, privacy and data-invasive products are put on the market, impacting people's lives well beyond the exercise of their rights and seeking to undermine the integrity of democratic processes.

In 2018, The Guardian revealed the unlawful and unethical relationship between Facebook and Cambridge Analytica, a controversial "data analytics" company.[8] In 2014, a group of social scientists led by Aleksandr Kogan created and deployed a personality test called "thisisyourdigitallife" via a Facebook app. This app allowed researchers to access personal information not only about app users but also their Facebook friends. These friends had not used the app and therefore could not have consented to the use of their data. This feature allowed Kogan and his team — along with potentially any other researcher with similar access — to harvest the information of a vast network of Facebook users. In the background, Global Science Research (GSR), Kogan's company, had contracted to disclose the data he collected to Cambridge Analytica, which had invested in advertising for the app. Cambridge Analytica analysed and used the data to create and purchase highly targeted ads that aimed to influence voters during the 2016 U.S. presidential elections and the Brexit referendum in the UK.

Cambridge Analytica replicated this method with other apps and surveys to get access to users information through other apps and surveys and then re-use the data to influence elections in Argentina, India, Mexico, Kenya, the Czech Republic and others. Cambridge Analytica for instance sought to influence the Nigerian presidential election in 2015 by using graphically violent imagery to portray a candidate as a supporter of sharia law who would brutally suppress dissenters and negotiate with militant Islamists.[9] In total, reports indicate that around 87 million people could have had their data used by Cambridge Analytica. While it is unclear if the propaganda techniques used by Cambridge Analytica translated into specific votes, the attempt to disrupt democracy via micro-targeting and data harvesting practices is clear.

Therefore, to protect democratic and electoral processes around the world, **the EU must pay very close attention to, monitor and report any data misuse in the context of its elections monitoring missions.**

This data scandal, which had clear global consequences, is the foreseeable result of an all too common business model: the widespread (over) collection and processing of personal information to create user profiles, in particular to generate better ad targeting. Users produce digital footprints at an alarming rate. Almost everything we do online or off can be — and often is –- tracked. With the dawn of the internet of things, this footprint is even bigger, and this means that companies are collecting and analysing troves of personal data at ever-increasing rates.

This scenario calls for a radical change in the way we enforce the protection of personal data. Contractual terms are not enough to provide adequate prevention, mitigation, protection, and redress even for normal use of a platform, much less for data misuse and abuse. The EU and its member states have a **responsibility to enforce data protection and privacy laws** to prevent and mitigate risks of data abu**se. Through its Action Plan, the EU should also promote the adoption of robust binding data protection laws** as well as encourage states to **ratify the Council of Europe Convention 108.** The Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data -- also known as Convention 108

[8] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[9] https://www.theguardian.com/uk-news/2018/apr/04/cambridge-analytica-used-violent-video-to-try-to-influence-nigerian-election

-- was adopted in 1980 and recently modernised.[10] Since its adoption, the Convention 108 was ratified by all 47 member countries of the Council of Europe, and by Mauritius, Senegal, Uruguay, and, most recently, by Tunisia and Mexico. Often considered as the mother of data protection law, the Convention 108 had a pivotal role in the adoption of the first Europe-wide data protection law in 1995 and the adoption of a large number of local and regional frameworks on data protection around the world.

The EU has an additional important role to play in the protection of privacy globally by adopting and implementing stronger rules and human rights protection for the selling of dual-use technology from the European Union to third countries. These rules are intended to cover a wide range of items that can surveil people's communications and moves, intercept mobile phones, remotely hack into computers and more. Authoritarian regimes around the world have used these tools sold by the EU to violate human rights, oppress citizens, silence political opposition, and attack human rights defenders.

The reform of the EU regulation on dual-use is still ongoing and while the EU Parliament has completed its Report, the Council of the EU is attempting to water down the law by pushing for weaker human rights protections. This is another area where the EU must protect people's human rights around the world and prevent harms. The future Action Plan should **recognise the need for stronger rules on the export of dual-use technologies** and **report on the use of technologies sold by an EU country to commit human right abuses and ensure access to remedy** for victims.

Human rights in the age of artificial intelligence and the EU's role

One of the main upcoming challenges for our digital societies will undoubtedly be related to the use and place of artificial intelligence (AI) in our lives. The concept of artificial intelligence encompasses a wide range of fields and processes without any widely agreed-upon definitions, either from a technological or legal standpoint. The current public debate surrounding AI can include everything from advanced algorithms and machine learning to the autonomous machines and robots. On a daily basis we are using advanced algorithms when we use search engines, credit ratings, voice and text recognition, instantaneous translations, job applications, autonomous vehicles, criminal justice, and more.

In the AI debate, both human rights but also the discourse around human rights, matter. They matter both from a perspective of identifying risks and harms as a source of solutions. While many of the human rights risks posed by AI are not new to the digital rights space, the scale at which AI can identify, classify, and discriminate among people magnifies the potential for human rights abuses in both reach and scope. AI-related human rights harms disproportionately impact marginalised populations primarily due to the fact that training data fed to AI systems reflects the marginalization of these groups throughout history. This bias is then reproduced in outputs that can entrench these patterns of marginalization.

As a first step to address this issue, Access Now, Amnesty International and other partners developed and published the **Toronto Declaration** on protecting the rights to equality and

[10] http://www.coe.int/web/conventions/full-list/-/conventions/treaty/108

non-discrimination in machine learning[11]. However, the right to non-discrimination is not the only human right implicated by AI. Human rights are interdependent and interrelated, and AI affects nearly every internationally recognised human right, from the rights to privacy and freedom of expression, to the rights to health and education.

Across the globe we are seeing examples of how artificial intelligence can be implemented in ways that can either benefit or hurt societies. Access Now published a report on **Human Rights in the Age of Artificial Intelligence**, where we look at the implications of the growth in AI-powered technologies through a human rights lens.[12]

In contrast to ethics, human rights are universal and binding, codified in international law and institutions, can provide well-developed frameworks for accountability and remedy. Where ethics lacks the means of enforcement, international human rights law possesses well-developed standards and institutions as well as a universal framework for safeguards. Ethical principles grounded in human rights can take advantage of this well-established structure to ensure that AI is developed, deployed and used in a manner that respects our fundamental rights.[13]

Universal human rights frameworks such as the Charter of Fundamental Rights are a cornerstone of our societies, helping to protect individuals online and off. International guiding principles such as United Nations Guiding Principles on Business and Human Rights have been developed for the implementation of human rights in the economy and they should be applied in the context of AI. It's imperative to embed these human rights frameworks in every aspect of the deployment of AI. The EU now has the potential — and the responsibility — to champion the **design, development and deployment of artificial intelligence to be individual centric and human rights respecting**.

To prevent and mitigate AI-related human rights risks we have made recommendations in four major areas:

1. **Comprehensive data protection legislation** can anticipate and mitigate many of the human rights risks posed by AI. However, in the context of AI additional measures may be necessary if they are not already present in data protection legislations.

- Notification: People must be notified if their data is used for automated decision making;
- Explanation: People should understand how and why an automated decision is made (purpose and logic used);
- Access and Correction: People should be able to access information collected about them and amend and modify information it if it is incorrect, incomplete, or inaccurate; and
- Objection: People should have the ability to contest the collection and use of their data.

---

[11] https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/

[12] https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

[13] https://www.accessnow.org/laying-down-the-law-on-ai-ethics-done-now-the-eu-must-focus-on-human-rights/

2. **Government use of AI should be governed by a high standard**, including open procurement standards, human rights impact assessments, full transparency, explainability and accountability processes.

- Follow open procurement standards: The procurement of any public-use AI system should be done openly, transparently, and include a period for public comment, with outreach to and meaningful consultation with potentially affected groups to ensure they have an opportunity to provide input.
- Conduct human rights impact assessments: Governments must thoroughly investigate AI systems to identify potential human rights risks prior to development or acquisition, including conducting an analysis on whether current law is sufficient to protect human rights.
- Ensure transparency and explainability: Maximum possible transparency about a system must continue throughout a system's life cycle, including development, conception and use.
- Establish accountability and procedures for remedy: There should always be a human in the loop, with significant oversight for high-risk areas.
- Develop redlines delineating contexts in which AI will not be used: Governments must draw and regularly re-examine guidelines for themselves in their use of AI to determine whether or no AI should be used in specific context based on human rights risks and societal impacts.

3. Given the **private sector's duty to respect and uphold human rights**, companies should go beyond establishing internal ethics policies and develop transparency, explainability, and accountability processes.

- Human rights due diligence: Potential rights-harming outcomes should be identified and effective action taken to prevent and mitigate harms, as well as to track the responses and provide avenues for remedy.
- Transparency and explainability: Private sector actors should endeavor to be as transparent as possible and provide meaningful information about how AI systems work.
- Accountability and remedy: Internal accountability mechanisms are needed and companies should ensure individuals have access to meaningful remedy and redress.

4. **More research should be conducted** into the potential human rights harms of AI systems and investment should be made in creating structures to respond to these risks.

The use of AI raise important societal challenges that should be addressed before rushing into the adoption of these technologies for the sake of innovation. Not every innovation means progress for society, especially if its impacts are not carefully considered and, if need be, mitigated. As we become aware almost daily of new discriminatory impact and human rights harms resulting from the use automated processes, the EU needs to ask itself which role it wants to play in the development of AI.

Developing smart AI regulation that keeps the human factor at the centre of the frame could and should be Europe's unique offer. This is not a simple gold rush—nor is it a doomsday scenario that requires iron-clad regulation across the board. Rather, every socially significant use of artificial intelligence should be assessed in context, critically judged for its effect on European

rights and freedoms, and regulated accordingly. While states and regulators may always be playing catch-up with technological change, that is no reason to cede the regulatory field. Human rights anchored legal principles that guide a better, more tailored AI offer are possible.

CONCLUSION

We appreciate the EU External Action Service openness in receiving inputs for the preparation of the future EU Action Plan on Human Rights and Democracy 2020-2024. We hope that our written comments contribute to the development of an EU digital strategy within the Action Plan and we look forward to continuing to work with you in the promotion of Human Rights within the EU and beyond.

We would appreciate the opportunity to come and present our views and recommendations in more detail in person at your best convenience.

Thank you,

Fanny Hidvegi
European Policy Manager
Access Now

Estelle Massé
Senior Policy Analyst
Access Now