ICNL

European Center for Not-for-Profit Law

PRESENTED TO **The U.N. Office of the Secretary General's Envoy on Technology**

JOINT SUBMISSION TO THE GLOBAL DIGITAL COMPACT CONSULTATIVE PROCESS

GDC Principles & Commitments

The International Center for Not-for-Profit Law (ICNL) and the European Center for Not-for-Profit Law (ECNL) are pleased to prepare this joint submission to contribute to the consultative process for the Global Digital Compact led by the U.N. Envoy for Technology and co-facilitated by Sweden and Rwanda. We appreciate this opportunity to set forth the principles and commitments that we believe are vital for an open, free, and secure digital future for all. We look forward to engaging with this process before, during, and following the Summit for the Future in 2024.

Connect All People to the Internet

CORE PRINCIPLES

Access to the global internet is integral to individuals' and organizations' ability to exercise their rights. The promises of government digitization efforts, online public participation, and expanding civic space are only available to those individuals who live in areas with internet connectivity and who can afford to pay the costs of connectivity, two factors which are out of reach for many. Lack of accessible and affordable internet exacerbates existing inequalities and exclusion of marginalized groups. Governments have a positive obligation to increase access and affordability for all people. Connecting all people to the internet is a prerequisite to the development and adoption of technologies for public services.

Government actions that hinder access, connectivity, and affordability including through the imposition of onerous taxes, internet disruptions, SMS censorship, and website and application blockages undermine the goal of utilizing the internet as a means of exercising fundamental rights. Orders to restrict access to the internet must be provided by law, necessary to advance a legitimate aim, and narrowly tailored to achieve that aim. Full or partial internet shutdowns are never proportionate. Internet shutdowns prevent a country's population from communicating with loved ones and accessing and sharing critical information.

KEY COMMITMENTS

Through the Global Digital Compact, States should recognize that meaningful access to the internet is a human right and a key means to access other fundamental economic, social, political, and civil rights. To this end, States should commit to adopting laws and policies that facilitate internet access and promote internet affordability. Such laws could establish tax incentives for third parties to provide more affordable internet services. States should invest in connectivity and institute programs like universal service funds that cover the costs of internet access for marginalized groups. States should also implement digital literacy programs to increase the capacity of all people to engage online meaningfully and safely. States should repeal existing laws and desist from introducing new laws that impose taxes on use of the internet or impose other onerous barriers to internet access. They should also commit not to pass laws or issue extralegal orders that disproportionately disrupt or throttle the internet, in whole or in part. Meanwhile, international financial institutions that are enabling States to invest in infrastructure development should ensure their loan instruments reflect rights-based obligations to reflect the commitments above.

Avoid Internet Fragmentation

CORE PRINCIPLES

The global, free, open, interoperable, secure, and reliable internet is critical for the protection of human rights and inclusive governance. A free, open, interoperable internet allows people from all countries to impart and exchange ideas. It is one of the key pillars of the global economy.

States and the organizations that create internet standards and protocols have made great strides in recent years to include participation of a broad range of stakeholders. Multistakeholder internet governance includes meaningful participation of ordinary citizens and representatives of marginalized and vulnerable groups. Multistakeholder internet governance is critical to ensuring that the internet is open, interoperable, free, inclusive, and safe.

KEY COMMITMENTS

States and multinational bodies should promote the principle of a global, free, open, interoperable, secure, and reliable internet both domestically and internationally. States should use international forums like the Internet Governance Forum to come to a common understanding of internet fragmentation at both the infrastructural and user levels, and develop policies that promote and protect a global, free, open, interoperable, secure, and reliable internet. Commitments should include prohibitions against intentional network disruptions that impact access to the internet in whole or in part, policies that promote the free flow of data across national borders in compliance with data protection principles, policies that promote network neutrality, prohibitions against the creation of national internet gateways or firewalls that segment the internet

through the use of either technical or policy frameworks, and policies that preserve universal standards for the operation of the internet.

Internet governance through domestic legislation, UN decision-making, and standard development organizations should include multistakeholder participation and enable civil society organizations, ordinary citizens, and marginalised communities to meaningfully participate in decision-making processes. It is not enough to state that a process is inclusive; these initiatives must invest in inclusion by increasing transparency of the processes, providing resources and opportunities for capacity building on technical issues related to internet governance, and making space for diverse voices to be heard.

Protect Data

CORE PRINCIPLES

Protection of personal data is essential to the right to privacy and serves as a pre-condition for other fundamental rights and freedoms (e.g., the freedom of assembly, association, and expression, both online and offline). Protection of personal data ensures that collecting and processing information about people, including activists, human rights defenders, and voters, is legitimate, transparent, and accountable. It prevents governments and companies from arbitrarily repurposing data for surveillance to stifle dissent or influence elections. In public spaces, it guarantees a reasonable expectation of anonymity necessary for participation in protests without the fear of repercussions. It is especially important in the digital age where privacy-violating technologies, such as remote biometric identification, are increasingly used to surveil and police people.

Core principles must include ensuring that data processing meets the requirements of necessity and proportionality and is based on an appropriate legal basis, established in primary legislation. Data minimization and purpose limitation should be enacted to guarantee that only data necessary for a specific purpose is processed and that data is not repurposed. All personal information must be secure and stored for a specified, limited time (no longer than necessary for fulfilling the purpose). Processing of data that reveals sensitive information, e.g., health, political views, sexual orientation, or ethnic background, should only be allowed in clearly defined situations.

Individuals should have access to effective rights, including the right of access to their data and information about processing, as well as redress mechanisms. When personal data is used as part of automated systems, individuals should have the right not to be subject to automated decisions, and oversight should be ensured by independent and well-resourced bodies.

It is also important to consider the societal dimensions (e.g., how data processing can impact groups of marginalised people, in addition to individuals within these groups).

Thus, the notion of a "vulnerable data subject" should be recognized as including both communities and individuals, and legal restrictions should be put in place restricting surveillance-based business models.

Finally, there should be no exemptions from the highest standards of data protection for public institutions, including law enforcement, national security authorities, and counterterrorism agencies.

KEY COMMITMENTS

States should adopt and promote strong personal data protection rules and create well-resourced, independent offices responsible for enforcement. States should actively protect encryption and anonymity, including by adopting laws, regulations and policies that confer only on courts the power to remove the right to anonymity, only when necessary and proportionate, rather than on law enforcement agencies. States should also commit to pushing back against national laws enacted by autocratic leaders for surveillance and censorship purposes which require telecommunication companies and online services to store citizens' personal data in the country.

To ensure low-resourced organisations, including civil society organisations, are well-placed to conform to data protection rules, States should commit resources and time to providing technical assistance and tools that better enable compliance prior to rules coming into effect.

Relevant UN human rights treaty bodies and special procedures mandate holders should enhance their synergies and cooperation, including through joint action, to strengthen data protection standards of relevant rights holders (e.g., Human Rights Committee, UNSR on Privacy and Data Protection and UNSR on Human Rights Defenders, UNSR on Counter-Terrorism and Human Rights, UN on the human rights of migrants, Committee on the Elimination of Racial Discrimination, etc.).

Apply Human Rights Online

CORE PRINCIPLES

The core principle that the same rights that apply offline also apply online should guide all components of the Global Digital Compact, and not be relegated to its own issue area. Furthermore, human rights protections should be the cornerstone of all online activities, either by public bodies or private entities.

It is crucial that all individuals' rights to privacy and non-discrimination, as well as the freedoms to expression, association, peaceful assembly, and other civic freedoms, are respected online. Individuals' online activity should not be subject to indiscriminate surveillance, including through blanket data retention obligations imposed on telecommunication companies and online services providers. Access to any online information by state authorities (be it data about internet users, their communications

or metadata like location or IP address) must be based on a relevant law, necessary and proportionate in a particular case, and subject to the authorization of an independent judicial authority. Individuals whose data was collected should be informed about this in due time and should have access to effective redress.

The export, import and deployment of invasive spyware, such as Pegasus, fundamentally violates the right to privacy and prevents people from exercising their rights to free expression and association. Spyware intimidates and silences activists, journalists and political opponents, undermining the very essence of democracy.

Finally, it is crucial that freedom of expression be safeguarded online, both by governments and by online services, especially the largest social media platforms which increasingly play the role of the digital public square, facilitating, but also at times curtailing, on their own initiative or on governments' requests, access to information and exchange of ideas.

There should be transparency of and judicial oversight over content take down requests or orders to online companies by public authorities. These orders should only be allowed when strictly necessary and proportionate and should be based on relevant primary legislation. Any removal or demotion of content posted by online platforms users, including social movements, activists, journalists, human rights defenders, should be compliant with human rights law, transparent, justified, and effective redress options should be available.

KEY COMMITMENTS

UN bodies and states should commit to push back against national laws that seek to limit fundamental digital rights and civic space, including national security laws, criminalisation of online activities, data localisation laws, censorship or content moderation laws. States cannot restrict human rights online, including freedom of expression, under the guise of "emergency measures". Any restrictions of human rights online must meet the relevant criteria established in the International Covenant on Civil and Political Rights (ICCPR) and other relevant human rights instruments.

States should, at minimum, impose an immediate moratorium on the sale, export, import and deployment of spyware technologies until a robust regulatory framework is in place. The regulatory framework on the proliferation of spyware technologies should, in line with calls of the European Data Protection Board, prohibit the development, use, and export of invasive spyware. Private surveillance companies should be legally obliged to disclose products and services offered and sold, including when using for national security and/or counter-terrorism purposes, and their clients.

UN bodies should enforce a robust, multi-stakeholder governance framework which empowers civil society and finances national and international watchdogs. These frameworks should be empowered through mechanisms such as import and export

controls or possibilities to sanction governments, companies, organisations, and individuals that do not abide by these principles.

The UN Tech Envoy should ensure a multistakeholder approach is implemented throughout the UN digital work and that civil society stakeholders are informed about the modalities of the negotiation and drafting process.

Large tech companies need to commit to maintaining safe spaces, making their tools available in recognized languages, upholding individual and collective rights, and addressing accessibility concerns. They should conduct human rights due diligence on their services, products and activities, including content policies, and ensure meaningful participation of civil society and affected communities. Effective internal grievance mechanisms should be established to appeal content decisions and other decisions affecting users. States should enact laws that grant users whose content was removed or demoted the possibility for redress with an independent judicial body.

Introduce Accountability Criteria for Discrimination & Misleading Content

CORE PRINCIPLES

Accurate identification of disinformation, hate speech or misleading content is extremely difficult and context-sensitive. Any measures aimed at tackling these issues must recognize this and ensure that free speech is not curtailed. Any limitations to the freedom of expression must be necessary and proportionate, must be based on clear criteria and objective assessment of illegality, and cannot lead to the criminalization of free speech. Overly vague and broad prohibitions of online content do not comply with Article 19 of the (ICCPR).

Examples of measures that do not comply with Article 19 include: criminalization of false information, disrupting access to entire platforms or websites for failing to comply with a takedown request, obligations to generally monitor all content on online services, requiring platforms to use algorithms to preemptively identify illegal or harmful content, imposing liability on platforms to take down content, particularly within excessively short deadlines. Such intermediary liability frameworks are likely to cause platforms to neglect their due diligence obligations and remove even lawful content in order to avoid legal responsibility, especially when this process is performed or supported by algorithms.

Online platforms' own content moderation policies must be enforced consistently and transparently. Takedown requests or orders by governments must be carefully assessed in light of relevant human rights laws and standards. Independent oversight by a judicial authority must be ensured for both voluntary content moderation by online platforms and take down requests or orders by state authorities. Finally, it is essential

to ensure meaningful transparency in reporting public authorities' requests for removal of online content and online services' compliance thereof.

KEY COMMITMENTS

Online platforms and States should develop and promote inclusive models and methodologies for risk and impact assessment of content curation and moderation, with meaningful participation of civil society and affected individuals and communities throughout the process.

States should commit to addressing the harms of online content only in ways that comply with their obligations under Article 19 of the ICCPR. The emphasis of State action should be on non-legal measures, such as media literacy programs, curriculum development for schools on how to critically assess information and news, and support to women and marginalised communities that are at greater risk of being targets for harmful content online. States should never criminalize posting or sharing false information online. States should only impose civil liability in cases where such information harms the rights or reputation of others; criminal penalties for defamation are not compliant with the ICCPR and should be eliminated. States should ensure that laws enable the investigation and prosecution of cyberstalking, online sexual harassment, online posts of non-consensual sexual images, and other forms of tech-facilitated gender-based violence and that law enforcement is equipped to investigate these incidents using trauma-informed practices. States should also commit to denouncing and investigating serious cases of incitement against marginalised communities by pursuing legal recourse on behalf of victims that have been harmed in accordance with recommendations in the Rabat Plan of Action. In cases when disinformation and/or misinformation threatens elections or other democratic processes, States should take a targeted approach to addressing these harms, such as through narrowly tailored rules on the use of algorithms and bots during political campaigns.

Regulations should require public authorities to publish regular reports with transparent information about their content takedown requests, including the number of requests, the type of requests, and their rationale. Such reports should also be published by online services, detailing how governments' requests for removal of content were assessed.

OHCHR, UN bodies and States must commit to identifying causes of disinformation and online harassment and addressing these issues through a variety of tools, not only technological ones. Any technological tools cannot lead to the curtailing of free speech or arbitrary assessment by private companies.

Promote Regulation of Artificial Intelligence

CORE PRINCIPLES

The use of AI must benefit individuals and society. Governance of AI systems must follow a human rights-based approach, guided by international human rights law and standards and relevant jurisprudence, rather than an ethics-based approach.

Regulation of AI must recognise that some forms of AI are incompatible with the international human rights framework, and prohibit the development and deployment of such systems, notably those that lead to mass (biometric) surveillance, discriminatory predictions, exploitation of people's vulnerabilities, and the undermining of rule of law and access to justice.

Consideration and assessment of human rights impacts must be embedded into every stage of the AI life cycle – from conception and design, through development and testing, to deployment and evaluation. These processes should meaningfully engage civil society and affected individuals and communities and their results should be made publicly available and accountable.

The development and deployment of AI must be transparent and accountable, especially in contexts with potentially severe impacts on human rights, such as law enforcement, migration, justice, national security, and counterterrorism. People affected by AI systems should be aware when AI systems are deployed, what their consequences are, and should have effective redress options. Information about the development or use of an AI system, including the assessment of the systems' impact on human rights, should be made public and should be subject to scrutiny by civil society, public interest researchers and well-resourced independent authorities.

Finally, regulatory frameworks on AI should not grant blanket exemptions from basic rules related to transparency, accountability, accuracy, and quality of AI systems on the grounds of national security and/or counterterrorism.

KEY COMMITMENTS

The UN should promote model AI governance to be established by both regulatory and co-regulatory standards at national and international levels.

Companies and public authorities, including all UN bodies, should conduct human rights due diligence to identify, prevent, mitigate and address violations of rights, including by undertaking human rights impact assessments when designing, developing or placing into the market their products and services as well as throughout their lifecycle.

Human rights impact assessments of AI systems should always include consultation with civil society actors and other experts and be validated by an accredited external independent oversight body with human rights expertise. UN bodies (e.g., OHCHR B-

Tech in coordination with OHCHR Civil Society Office) should facilitate an ongoing multi-stakeholder dialogue, in particular between AI systems providers and civil society organisations, in order to foster trust, accountability and cooperation.

The UN Tech Envoy office has an important position in relation to private-sector actors, particularly information communication technology (ICT) companies and their engagement with the U.N. via public-private partnerships. Tech Envoy is well-placed to ensure the transparency of private-public partnerships the UN enters into, as a model for other international, regional, and national bodies.

UNESCO should implement more transparent and open approach to implementing the Recommendation on the Ethics of AI, including engagement with broader civil society actors on both monitoring and implementation of the Recommendation, especially within impact assessment processes and its piloting on a member state level.

UN CTED and OCT should implement more transparent and open approach to developing and implementing the UN Global Counter-Terrorism Strategy, including engagement with broader civil society actors on both monitoring and implementation of the Strategy and relevant instruments.

Any technical standard-setting bodies, including the ITU, should commit to ensuring an open and inclusive standardization process available to civil society and human rights experts. Any standards must comply with the international human rights framework.

About ICNL and ECNL

EUROPEAN CENTER FOR NOT-FOR-PROFIT LAW

ECNL is a civil society organization based in The Hague, The Netherlands, with 20 years of experience in building and advocating for better legal and policy environments for civic groups, movements, and activists. It creates knowledge and works with partners to set global and regional standards to protect and expand civic freedoms online and offline. It focuses on global drivers that affect these freedoms and the complex needs of civil society, including the need to streamline fundamental rights safeguards in the development and functioning of technology and AI systems and devices.

When it comes to addressing the impact of technology on civic space, ECNL builds bridges between policy makers, academics, and industry on the one hand and non-digital-rights civil society organizations, including representatives of marginalized and vulnerable groups, on the other. It also engages in advocacy related to global, regional, and national laws and policies related to AI and emerging technologies, including the EU AI Act and the Council of Europe Framework Convention on AI. ECNL is a member of the Global Internet Forum to Counter Terrorism and the Financial Action Task Force Private Sector Consultative Forum, an affiliate of the European Digital Rights initiative (EDRi) and the representative of the Conference of

International Non-Governmental Organisations (CINGO) of the Council of Europe's Committee on Artificial Intelligence.

INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

ICNL is an international not-for-profit organization that promotes an enabling environment for civil society and public participation worldwide. ICNL has provided technical and research assistance to support the reform of laws affecting CSOs in more than 100 countries. ICNL's small but capable international staff includes experts in all aspects of the laws governing the freedoms of association, assembly, and expression, and right to privacy, offline and online.

For over a decade, ICNL has been working at the intersection of digital rights and civic space by supporting local leadership and capacity to counter extralegal, vague, and disproportionate civic space restrictions. We have worked with UN Special Rapporteurs (UNSRs) to create international standards on internet shutdowns, disinformation, and surveillance technologies, we have engaged with the UN Office of the High Commissioner for Human Rights (OHCHR) to increase protections for civic space online through UN resolutions and treaties, and we are a member of the Freedom Online Coalition (FOC) Advisory Network. ICNL has also sought to empower local partners on a wide range of digital technology and civic space issues via an annual Tech Camp we co-host with the Global Digital Policy Incubator at Stanford University.

Due to our work at the international and national levels, ICNL is recognized as an expert on many issues at the intersection of technology and civic space. In 2012, ICNL received a MacArthur Award for Creative and Effective Institutions in recognition of its work to create an enabling environment for civil society worldwide.

For any questions about the submission or to discuss the principles and commitments outlined in this document in more detail, please email INCL's Senior Legal Advisor Zachery Lampell at zlampell@icnl.org and ECNL's Digital Civic Space Advisor Karolina Iwanska at karolina@ecnl.org.