SUBMISSION OF INPUTS FOR THE GLOBAL DIGITAL COMPACT

April 30, 2023| India

I. Introduction

The Council for Social and Digital Development (CSDD), the Digital Empowerment Foundation (DEF), the North East Development Foundation (NEDF), and the Royal Global University (RGU), Assam, and the eNorth East Digital Alliance, is pleased to submit inputs to the Global Digital Compact (GDC). The inputs are based on a VWDNHKROGHU¶V discussion from the North East Region of India in South Asia (comprising of 8 States covering the North East India Himalayan States), through online mode (Zoom meeting) on April 28’ 2023. The discussion was on the state of connectivity and the social aspect to digital access and technological advancements with a focus on north east Indian states, the geographical spread of which greatly overlaps with the eastern Himalayan region

go. It is not internet alone but all the supporting infrastructure of regular electricity supply, last mile networks, access to devices needs to work in congruence as an integrated toolkit.

Satellite Connectivity as a key priority: Cost of accessing internet connectivity will come down in the next few years with the proliferation of satellite connectivity. But reliance on physical infrastructure like towers, fiber is going to be counterproductive.

Meaningful connectivity and affordable connectivity : should be guiding factors to PDNH µ,QWHUQHW IRU DOO¶ D UHDO SRVVLELOLW\ 7KLV
significance.

Internet and digital training

Promoting digital literacy: To make sure that everyone has the skills and information required to use the internet efficiently and safely, civil society organisations, governments, and businesses should encourage digital literacy programmes.

Accessibility: Businesses and governments should endeavour to ensure that everyone has inexpensive access to the internet, especially those who live in rural or low-income areas.

Ensuring user privacy and security: When connecting consumers to the internet, governments and businesses should prioritise their privacy and security. This can be accomplished by rules, guidelines, and instruction on safe internet usage.

Fostering innovation: To broaden access to the internet and enhance its capabilities, businesses and governments should support innovation and the creation of new technologies.

Collaboration with stakeholders: To accomplish the aim of universal internet access, all stakeholders ² including schools ² should cooperate and work together. Partnerships between governments, businesses, and groups from civil society are examples of this, as well as interactions with nearby communities and educational institutions to learn about their wants and requirements.

2. Digital commons as a global public good

Core principles

The following are some of the core principles for digital commons as a public good:

Accessibility: Digital commons should be easily accessible to everyone, regardless of their background, income, or social status. This includes access to digital infrastructure, tools, and services that enable people to participate in the digital commons.

Openness: Digital commons should be open and transparent, allowing for free access, use, and modification of the digital resources. This includes open data, open-source software, and open educational resources.

Collaboration: Digital commons should be based on collaborative and participatory models of production, where individuals and communities work together to create and maintain shared digital resources.

Sustainability: Digital commons should be sustainable over the long term, with a focus on maintaining and improving the quality of the digital resources for the benefit of current and future generations.

Diversity: Digital commons should be diverse and inclusive, reflecting the needs and perspectives of different communities and cultures. This includes promoting cultural diversity, linguistic diversity, and gender diversity.

Privacy and security: Digital commons should be designed with strong privacy and security measures to protect users' personal data and prevent unauthorized access or misuse of digital resources.

Democratic governance: Digital commons should be governed in a democratic and transparent manner, with clear and fair rules for decision-making, participation, and accountability.

Key commitments

Transparency: Institutions, businesses, and other parties involved in decision-

Governments should refrain from making digital sovereignty decisions which lead to internet fragmentation.

4. Promote regulation of artificial intelligence

Core principles

Transparency: AI systems should be designed and developed in a transparent manner so that users and stakeholders can understand how the system works and make informed decisions about its use.

Accountability: Developers, users, and other stakeholders should be held accountable for the impact of AI systems on individuals, society, and the environment.

Fairness: AI systems should be designed and developed in a way that is fair to all individuals and groups, regardless of their race, gender, religion, or other characteristics.

Safety and security: AI systems should be safe and secure, and designed to minimize the risk of harm to individuals and society.

Privacy: AI systems should be designed and developed in a way that respects individual privacy and data protection.

Human -centered de sign: AI systems should be designed to enhance human capabilities and support human well-being.

Ethical considerations: Developers and other stakeholders should consider the ethical implications of AI systems, including issues related to bias, discrimination, and human dignity.

tions:

Key commitments

Government:

a) Develop and implement clear policies and regulations that guide the development and deployment of AI technologies.
b) Establish a framework for ethical considerations in AI development and use.
c) Foster collaboration between government, industry, academia, and civil society to

d) Foster collaboration with other stakeholders to ensure that the benefits and risks of AI are adequately assessed and addressed.

e) Encourage transparency and accountability in the development and deployment of AI technologies.

Research Agencies:

a) Conduct research on the societal and ethical implications of AI technologies.

b) Develop and promote standards for the development and deployment of AI technologies.

c) Foster collaboration between researchers, industry, and civil society to ensure that the benefits and risks of AI are adequately assessed and addressed.

d) Conduct independent evaluations of AI technologies to ensure that they are safe, reliable, and effective.

e) Develop and promote ethical guidelines and a framework for the development of AI technologies.

Civil Society:

a) Advocate for transparency, accountability, and ethical considerations in the development and deployment of AI technologies.

b) Monitor and evaluate the use of AI technologies to ensure that they are fair and do not perpetuate discrimination or inequality.

c) Foster collaboration with other stakeholders to ensure that the benefits and risks of AI are adequately assessed and addressed.

d) Promote public awareness and education on the societal and ethical implications of AI technologies.

e) Encourage the development and use of AI technologies that benefit society as a whole.

5.

Transparency: Businesses should be open and honest about how they gather, store, and use data. They should give people access to their own data and be transparent about the data they acquire, how they use it, and what they do with it.

Consent: Before collecting or processing a person's personal information, businesses should get that person's express consent. This consent must be freely given, precise, well-informed, and clear.

Data security: To prevent unauthorised access to data, businesses should put strong data security procedures in place. They ought to create access controls, encrypt important data, and periodically assess their security procedures.

Data minimization: Businesses should only gather and use the data required for the services they offer. They should refrain from gathering superfluous data and remove it once it is no longer required.

Accountability: Parties responsible for data breaches or misuse should be held to account, including businesses, governments, and other entities. They should be obligated to take immediate action to mitigate any harm caused by breaches and promptly report them.

Education: Governments, businesses, and civil society organisations should collaborate to educate people about data privacy and security and equip them with the tools they need to do so.

Collaboration: Governments, companies, civil society, and other organizations should collaborate to develop and implement effective data privacy and security policies and practices.

6. Apply human rights online

Core Principles

Respect for the rule of law: All stakeholders should respect the rule of law and ensure that human rights are protected and upheld online in the same way they are in the offline world.

Accessibility: Stakeholders should ensure that everyone has equal access to the internet and digital technologies, regardless of their background, socioeconomic status, or geographical location.

Privacy: All stakeholders should respect and protect individuals' right to privacy online, including their personal information and data.

Freedom of expression: Stakeholders should protect and promote freedom of expression online, while also addressing any harmful content or behavior that may threaten this right. Policy should define the severity of an expression online.

Digital literacy: Stakeholders should promote digital literacy and education to help people understand their rights and responsibilities online, including how to protect themselves and others from online harm. Self-regulation is equally important as part of this literacy.

Non-discrimination: All stakeholders should ensure that people are not discriminated against online based on their race, gender, sexual orientation, religion, or any other characteristic.

Transparency and accountability: Stakeholders should be transparent about their actions and decisions related to online human rights and be accountable for any violations that occur.

Key Commitments

Protecting the right to privacy: Governments and companies must ensure that individuals have the right to control their personal data and information, and that their privacy is respected.

Protecting freedom of expression: Governments must ensure that individuals have the right to express themselves freely online without fear of censorship or retaliation.

Ensuring access to information: Governments and companies must ensure that individuals have access to information that is necessary for them to participate fully in society, such as news, education, and health information.

Preventing online harassment and abuse: Governments, companies, and civil society must work together to prevent online harassment and abuse, and to hold perpetrators accountable. New techs can be leveraged to identify violation of basic access to expressing opinions online.

Respect for diver sity: Online material should respect diversity by not discriminating against or marginalising people or groups based on their ethnicity, gender, religion, sexual orientation, or handicap.

Ethical standards: Creators and publishers of online content should adhere to ethical standards for journalism and communication. This includes respecting privacy, avoiding sensationalism or clickbait, and avoiding plagiarism.

Key commitments

Commitment to Transparency: All stakeholders, including content creators, publishers, and platforms, should commit to transparency about their content creation and distribution processes. They should clearly state their policies on what constitutes misleading or discriminatory content and how they plan to enforce these policies.

Promoting Education and awareness: All stakeholders should work to educate themselves and others about the harms of misleading and discriminatory content. This includes training content creators, publishers, and platforms on how to recognize and address such content, as well as educating the public on how to identify and report misleading or discriminatory content.

Ensuring Enforceability: All stakeholders should commit to enforcing their policies on misleading and discriminatory content. This includes taking action against content creators and publishers who violate these policies, such as removing their content from platforms and holding them accountable for any harm caused.

Commitment for Collaboration: All stakeholders should work together to address the problem of misleading and discriminatory content. This includes sharing best practices, collaborating on research, and developing tools and technologies that can help identify and remove such content.

Willingness and capacity for Continuous improvement: All stakeholders should commit to continuously improving their policies and practices around misleading and discriminatory content. This includes regularly reviewing and updating their policies to reflect changes in the media landscape, as well as investing in research and development to identify new ways to address the problem.

Stakeholders Discussion Panel Members

1. Atreyee Borooah Thekedath, Founder CEO, Webcom (India) Pvt Ltd
2. Dr. Bhogtoram Mawroh, Senior Associate, Research and Knowledge Management, North East Slow Food and Agrobiodiversity Society (NESFAS)
3. Dr Anupam Das, Associate Professor & Co-ordinator, RSIT
4. Dr Ishita Chakraborty, & Associate Professor & Co-ordinator, RSET
5. Dr Aruna Dev Rroy, Associate Professor, RSC
6. Jayanta Deka, Digital Editor, The News Mill
7. Dr. Kaberi Bezbarua, Assistant Professor, Accountancy, Gauhati Commerce College
8. Karma M. Bhutia, Founder, Demi Solutions
9. Ninglun Hanghal, Freelance Journalist based in Imphal, Manipur
10. Sanjib Sarmah, OSD, Assam Electronics Development Corporation Limited (AMTRON)
11. Sanjeev Sarma, Founder Director & CEO, Webx Technologies
12. Dr. Syed S. Kazi, Director, Council for Social and Digital Development
13. Dr. Y. Jayanta Singh, Executive Director, National Institute of Electronics & Inf Tech. (NIELIT), AFC Building, Paltan Bazar, Guwahati - 781008, Assam

****