Youth for Privacy’s written input to the third substantive session of the Open-ended Working Group on security of and in the use of information and communications technologies

Youth for Privacy is a youth-led and youth-centered group advocating for privacy. Our goal is to make privacy a fundamental and accessible value throughout all levels of society using practical methods. By bringing together privacy-minded youths around the world, we aim to make focused, tangible change in the field of information and communication technologies.

For discussion on best practices and lessons learnt with regard to stakeholder involvement in capacity-building initiatives in the ICT security sphere.

Thank you Distinguished Chair. My name is Adamma Izuegbunam Chau, representative for Youth for Privacy. I am a millennial born in the same year the World Wide Web launched into the public domain. Since then, ICTs including contemporary artificial intelligence have grown increasingly embedded into our daily lives whether we know or consent to its applications.

Youth for Privacy is a global group that makes the often invisible value of privacy visceral with the next generation of privacy-minded youth. Learning from our work in youth advocacy and consensus building, we recommend member states secure ICT for youth with the following best practices:

1. Amplify youth voices within the cyber sphere. We have seen how operating in silos creates gaps and redundancy. Shrink the multigenerational divide by supporting our efforts, and trust us to speak to our own insights. Commit to a dedicated youth-led session with accessible means of participation in the next substantive working group. Consistent engagement beyond ad-hoc events is necessary to sustain meaningful contribution.

2. Build with an intersectional framework by centering the youth beyond cyber spaces. While YFP is primarily made up of people who grew up with relatively easy access to ICTs, we know that is not the case for 63% of young people globally. Understand specific matters
concerning young populations who 1) have limited safeguards against public ICT and 2) do not directly use ICTs, but are impacted.

Multiply-marginalized youth are also often disafforded physical and psychological safeties of privacy autonomy. Transgender-disabled Black and brown youth, especially, are more likely to encounter cyberbullying and search for physical and mental health support online compared to their counterparts.

Co-create youth education programs on secure internet use to encourage a broad range of youth participants at the systematic level. Education in all technical and non-technical fields must promote privacy education, i.e. awareness of information flows and purpose of data collection across all sectors. Produce these learning materials with standards like Cyber Collective. Goals should be objective oriented with associated metrics.

3. Bolster policy to reduce harm. Endorse negotiations for a comprehensive cybercrime treaty that demands the inclusion of human rights standards to guarantee full protections for youth. Refine existing goals in your domain to realize The 2030 Agenda for Sustainable Development and other models. This includes technical decision makers prioritizing students' privacy over short-term incentives in the long-term adoption of e-learning technologies accelerated in the COVID-19 pandemic.

Thank you and we look forward to continued conversations in the next substantive session.

For discussion on how stakeholders can work together with States to contribute to the implementation of the concrete, action-oriented proposals made by States at the first and second substantive sessions of the OEWG.
Thank you honorable chair. Good afternoon distinguished delegates and fellow stakeholders. My name is Amogh Dimri, I am a representative of Youth for Privacy.

These past two days of negotiations have made clear that this body believes cyberterrorism and cyberattacks are central threats in the effort to foster safer ICTs. However, we the youth believe an equally important yet largely overlooked threat to that future is the affront to individuals' private data occurring everyday. In fact, it is the normalized corporate data mining and sale of individuals' private data without public awareness that we wish to rectify.

Youth for Privacy is a collective of youth from around the world advocating for privacy as a human right and empowering more passionate youth to join our advocacy efforts. Our efforts to ensure the youth voice is heard on the issue of ICTs is not only because users aged 18 to 24 comprise a quarter of global internet usage but also because today's youth come from a generation that has grown up with the internet for their entire life. And will see the internet, and new technology like artificial intelligence, become increasingly pervasive and define the rest of their lives in an unprecedented manner.

In Section F, the progress report discusses Capacity-Building for future discussions on ICTs as potentially offering new cooperation between States and concerned Stakeholders. Furthermore, the Recommended Next Steps in Section G on Regular Institutional Dialogue calls for new mechanisms to advance capacity building. To these ends, we the youth assert there is no more pertinent stakeholder perspective and no better way to bolster this working group's capacity-building efforts for the next session than to sponsor an international cohort of youth delegates to attend the fourth and fifth sessions of this working group. We seek to have youth be involved in the decision-making process regarding data privacy and to be heard during the working group's discussion that will shape the internet for their entire lives. Youth for Privacy is eager to aid this body in reaching out to

youth passionate about data security and privacy to help build a rounded discussion on internet security with a robust and involved youth presence in future sessions.

Secondly, we wish to remind states that with respect to Section D concerning International Law, the right to privacy is enshrined in The Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Convention on the Rights of a Child. They read: "No one shall be subjected to arbitrary [or unlawful] interference with his or her privacy." So, if privacy is a human right protected by international law, then why do we ignore the routine and normalized breaches of individual data privacy and instead exclusively highlight cybercrime as a threat. The right to privacy is an essential and core right for all, especially with regards to women's and children's rights. And going forward, we youth assert that the internet will become the new battleground for our right to privacy. With this in mind, the progress report must be expanded to herald the right to privacy as a core directive for states to uphold online with the same vigor they do in the physical world. We urge this body to highlight the right to privacy under international law in the progress report as a reminder to states that protecting this right is essential for any future discussions on ICTs.

Finally, we urge states to expand upon Section C of the progress report on “Responsible State Behavior” with a privacy review stage that comes before implementing cybersecurity responses. This will prove crucial in ensuring an individual's privacy was not impeded on by such measures. Privacy is, after all, a human right and therefore, there can be no such a thing as responsible state behavior on this issue of ICTs without giving credence to existing international law regarding privacy.

I thank you for your time, and am eager to work with fellow stakeholders and member states. To further the goal of protecting privacy and continue to empower youth voices on ICT discussions.