Oral statement on groups 6-10

Global Partners Digital

Delivered by Ellie McDonald, Global Advocacy and Engagement Lead
Friday, 25 August 2023

Chair, distinguished delegates, thank you very much for this opportunity to share the views of Global Partners Digital or GPD. I will share some brief remarks on Articles 6-10, Article 28 and Article 36 and refer to GPD's written submission for our full analysis.

Regarding Articles 6-10, we wish to reiterate our recommendation that the future convention should only include the core cybercrimes which it is intended to cover—that is articles 6 to 16.

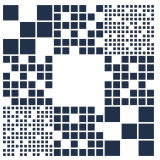
While supporting the inclusion of Articles 6-10, we note that—as drafted—these articles risk undermining the purpose of the future convention by chilling critical cybersecurity work. Across these articles, there is a need to incorporate a heightened standard of intent and a clear and expansive public interest defence to ensure that the work of journalists, whistleblowers and security researchers is not captured.

In addition, we note that, without a proper public interest defence, Article 12 could be interpreted as providing the grounds to criminalise the action of whistleblowers and journalists who access information or personal data and share it in the public interest—their activities are protected under freedom of expression and the public's right to know and should not be captured by the future convention.

We appreciate that Article 6(2) and Article 10(2) seek to provide some defence against over-criminalisation, however the current language is inadequate to mitigate the risks. We recommend Article 6(2) is strengthened to make infringing security measures a mandatory rather than an optional requirement, and that the word "authorised" be deleted from Article 10(2).

Turning to Article 28 on search and seizure of stored [computer data] [digital information], we note with concern that this provision could be interpreted as incentivising the adoption of disproportionate measures, such as demanding the handling of encryption keys or disclosure of security vulnerabilities that enable the stockpiling of vulnerabilities and facilitate surveillance.

Collectively, we believe that, Articles 6-10 in their current wording, and Article 28, rather than making us more secure, risk making us less so by chilling critical cybersecurity work and incentivising the use of measures which compromise the security of digital communications



and services. We encourage states to consider the above modifications to Articles 6-10 and the removal of Article 28.

Finally, we wish to highlight our support for **Article 36** on the protection of personal data. Robust provisions on data protection are essential to the success of the future convention as they can safeguard human rights and facilitate international cooperation. For this to be achieved, the provision should provide clear standards for the transfer of personal data.

We recommend that this provision is strengthened by explicitly referencing that personal data transferring conditions should fulfil international human rights standards, and by referring to recognised data protection principles, such as lawful and fair processing, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

I thank you for your attention.