Access Now's statement to the third session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes

Item 4 - Provisions on International Cooperation
31 August 2022

Delivered by Laura O'Brien (Senior UN Advocacy officer)

[Check against delivery]

Chair, we thank you for this opportunity to speak at this third session of the Ad Hoc Committee.

We recognise the importance that international cooperation plays in addressing cybercrime and that for many states, this issue is one of the main motivators behind their involvement in this process. As we noted in our submission prior to the second session, while international cooperation measures are crucial, they can also have the danger of adversely impacting the rights to privacy, data protection, and other fundamental human rights.

Any international legal framework on cybercrime cooperation must therefore ensure appropriate legal standards, accountability, remedy, authentication, and oversight in legal assistance - including a clear role for judicial institutions. States participating in any such framework must commit to public transparency reporting with clear, easily accessible information covering the way users' data records are shared amongst law enforcement across jurisdictions and by notifying users when their data are accessed. Such requirements must be put in place for all data sharing and international cooperation relating provisions that might be included in the proposed treaty. Such "transparency reporting" requirements have now become a global best practice with respect to regular periodic disclosure by technology and telecom firms, as well as by some governments. It must therefore be included in the proposed treaty.

The treaty should not seek to go into criminalisation of personal data, noting that this also pertains to the earlier agenda item on criminalisation in the second session. The sections on international collaboration and any cross border data transfers must include safeguards on personal data.

We note that the conversation appears to be still taking place between states whether international cooperation and data sharing related provisions should cover all crimes, or only those specifically included in the treaty. Many states have indicated that provisions on criminalisation should focus

mainly or solely on cyber-dependent crimes. We therefore reserve the right to provide additional views on this in the near future. We do hold the initial view that the best way forward for the Ad Hoc Committee may be to ensure that data sharing initiatives adhere to principles of dual-criminality, proceed in writing under standard protocols, and raise, not lower, protections against arbitrary or unlawful interference. Any proposed treaty should ensure that states retain the rights to refuse any legal assistance or data disclosure request on grounds relating to human rights or concerns from the state that it pertains to a political offense.

We recommend that the Ad Hoc Committee adopt the definitions and procedural safeguards outlined in the International Principles on the Application of Human Rights to Communications Surveillance (also called the "Necessary and Proportionate Principles"). That includes avoiding legacy legal definitional approaches such as metadata versus content data, and instead adopting the term “Protected Information” as a technology-neutral standard. As the Necessary and Proportionate Principles further explain, this approach avoids outmoded models of binary classification, and also recognise that in some cases persistent, widespread collection of data that would otherwise not be treated individually as protected information can in fact rise to the threshold of legal concern due to technology or intrusive techniques revealing private information in excess of the individual parts of such data.

In 2015, we published a Universal Implementation Guide for the Necessary and Proportionate Principles, which provides a detailed, step-by-step guide to creating a legal authorisation and disclosure process for data requests focusing on a four-part process: (1) the initiation of the surveillance request, (2) the court order authorizing such surveillance, (3) the communication providers response, and (4) the execution of the surveillance order. We believe that judicially approved warrants must be the normal, baseline standard for how information can be accessed via communications surveillance, not executive controlled or supervised processes. We caution that any other approach would fall short of meeting the standards increasingly recognised in international human rights law and the lessons learnt from surveillance oversight failures in many countries.

We will make available our universal implementation guide and additional resources to the Ad Hoc Committee.

Thank you Chair, delegates.

—