Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Cybercrime Convention Negotiations

Microsoft's submission to the Sixth Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Microsoft is grateful for the opportunity to contribute to the Ad Hoc Committee (AHC) efforts to develop a cybercrime convention. In line with our previous submissions, we believe the success of these negotiations and the effectiveness of the resulting convention depend on narrowly defined scope and consensus-based agreement. The new convention should therefore apply only to serious offences defined in the text. It should focus on addressing cyber-dependent crimes and refrain from introducing expansive procedural or international cooperation provisions that could lead to conflict of laws, jurisdictional disputes, human rights violations or weakened national security.

In our experience, cybercriminals often operate across borders and as a result international cooperation needs to be at the core of any new global treaty on countering cybercrime. However, this cooperation must be based on predictability and trust, and can only be achieved if the offences and powers set forth in the convention are commonly understood and applied transparently by all parties involved. Government access to data should be limited to cybercrime offences defined in this convention and meet specific public safety and national security requirements. We likewise urge states to limit the procedural powers to serious crimes defined in this convention and to provide clear guidance on jurisdiction to avoid disputes. The rights of end users of digital products and services should also be protected by incorporating robust human rights safeguards, independent oversight, and effective redress mechanisms for victims.

In line with the above, we provide detailed comments on individual chapters contained in the Zero Draft below. However, as a matter of priority, we believe states should:

- **Align the convention with existing instruments and data protection standards** to avoid conflict of laws, confusion, delays, increased costs, and potential cooperation breakdown.
- **Criminalize core cybercrime offences** such as illegal access to computer systems while focusing on serious crimes to streamline processes.
- **Limit the scope of provisions**, particularly those on data access, to a narrow set of crimes clearly defined in this convention.
- **Avoid expanding the definition of cybercrime** to encompass online content, undermining human rights, such as freedom of expression and the right to privacy.
- **Incorporate human rights safeguards**, such as independent oversight, right to appeal, and effective redress mechanisms to minimize conflicts with international human rights law.
- **Exempt ethical hackers and cybersecurity researchers** from the scope, including by requiring "*criminal intent*" to establish offences under this convention.
- **Streamline requests for e-evidence**, including by limiting government access to data that is necessary for specific public safety and national security needs and by directing demands to "*data custodians*".
- **Preserve the right of technology providers to challenge government demands** for data on behalf of their customers.
- **Increase transparency** by allowing data custodians to give notice to users when their data is requested, unless doing so might compromise an ongoing investigation.
- **Clamp down on "safe havens"** by strengthening extradition measures to ensure cybercriminals cannot evade prosecution and accountability.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

Detailed comments on Zero draft of the UN convention on countering cybercrime

Our understanding is that the sixth substantive session of the Ad Hoc Committee, in August 2023, will focus on the zero draft text of the convention, including on the preamble, general provisions, criminalization, jurisdiction, procedural measures, international cooperation, preventive measures, technical assistance, the mechanism of implementation, and the final provisions. This submission responds to key elements contained in each chapter and builds on Microsoft's submissions to the fourth and fifth substantive sessions, which looked at similar issues.

Preamble

We understand that many states prefer to make decisions on the preamble text only after key substantive provisions, such as those related to scope, criminalization, procedural measures, and international cooperation, have been agreed upon. Microsoft supports this approach but urges states to **balance criminal justice needs with the legitimate interests and rights of users** of ICT products and services. We also recommend that states ensure the convention remains future-proof, does not undermine human rights and fundamental freedoms, or produce unintended consequences for legitimate online activities. In line with this, we propose states:

- **Reintroduce agreed UN language on human rights online** which was present in a previous version of the preamble. The deletion of agreed human rights language, particularly by a subsidiary body of the 3rd Committee of the UN General Assembly charged with safeguarding human rights, raises serious concerns and sets a dangerous precedent for future backsliding.
    - **PP.2(bis):** *"Committed to promoting an open, secure, stable, accessible and peaceful cyberspace for all, where the application of international law and fundamental freedoms are promoted, and human rights are protected."*
    - ***PP.11:*** *"Mindful of the need to achieve law enforcement objectives and to ensure respect for human rights and fundamental freedoms as enshrined in ~~applicable~~ existing international and regional instruments, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning respect for privacy."*
- **Protect the legitimate interests of users of ICTs**, be it governments, private sector entities, civil society organizations, or individuals by amending the preamble as follows:
    - ***PP.9:*** *"Recognizing the need for cooperation between States and relevant non-governmental organizations, civil society organizations, academic institutions and the private sector in combating cybercrime to protect the legitimate interests of users of information and communication technologies."*
- **Future-proof the convention** by, inter alia, deleting selective enumeration of existing challenges:
    - **PP.3:** *"Concerned that the use of a computer system can have a considerable impact on the scale, speed and scope of a variety of criminal offences~~, including offences related to terrorism, trafficking in persons, smuggling of migrants, illicit manufacturing of and trafficking in firearms, their parts, components and ammunition, drug trafficking and trafficking in cultural property,~~*

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Chapter I. – General Provisions

From Microsoft's perspective, the convention should combat cybercrime by facilitating international cooperation while **protecting the confidentiality, integrity, and availability of user data** and essential digital services. This can be achieved by avoiding unchecked digital surveillance and by clearly defining the purpose and scope of the convention. The convention should be limited to a precisely defined set of crimes and include appropriate human rights safeguards, robust independent oversight, and effective redress mechanisms. It should also minimize conflicts with existing laws and create mechanisms to resolve any disputes that might arise. Broadening the scope of this treaty beyond countering traditional cybercrime risks undermining existing efforts to combat this threat and could also result in unintended negative consequences for legitimate online activity, negatively impact human rights, and undermine national security. In line with this, we propose that states:

- **Balance criminal justice needs with protection of users of ICT services** by amending the convention's statement of purpose as follows:
    - **Art.1(a):** *"Promote and strengthen measures to prevent and combat [cybercrime] more efficiently and effectively while protecting users of information and communications technologies from such crime;"*
- **Limit the application of measures in this convention to a precisely defined set of crimes** to ensure predictability and avoid conflict of laws, jurisdictional disputes, and breakdown of international cooperation in this space. A broad global data access treaty under the guise of fighting cybercrime, as currently envisioned by Article 3 on the Scope of Application, would inevitably clash with existing data protection standards and undermine trust in the digital ecosystem.
    - ***Art.3(2):*** ***"****This Convention shall also apply to the collecting, obtaining, preserving and sharing of evidence in electronic form for serious criminal offences established in accordance with articles 6 to 16 of this Convention, as provided for in the relevant articles of this Convention.*
- **Streamline requests for e-evidence by directing demands to "*data custodians*"**. With an increasing number of organizations relying on cloud computing, law enforcement agencies often have multiple data sources at their disposal. Whenever possible, digital evidence should be obtained from the "*data custodians*", which are the most proximate source of the data. In many cases this will not be the cloud or service provider. Going directly to the data custodian can often be done without jeopardizing an investigation, just as it was the case before organizations moved their data to the cloud. Doing so will also expedite data access requests, producing better results. To that end, we propose to replace the term "*service provider*" with "*data custodian*" throughout the text and replace the existing definition in Article 2 on the Use of Terms with the following text:
    - **Art.2(e)(i):** *"~~Service provider~~ Data custodian shall mean: Any legal or natural person, agency, public authority, service provider or any other body who acts as a controller for the purposes of collecting, holding, processing or accessing personal information which is the object of a request for cooperation under this Convention."*

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

Chapter II. – Criminalization

Microsoft reiterates that for the convention to be effective, the technology industry and data custodians must have **a clear understanding of what constitutes a cybercrime** to be able to respond appropriately to government requests for electronic evidence. This requires criminalizing only cyber-dependent offenses and not expanding the scope of procedural and international cooperation measures to all crimes merely because a computer was involved.

We also urge states to recognize that their diverging political, cultural, and legal systems may prevent them from reaching a common understanding of what constitutes serious criminal "*offenses committed by a means of a computer system*". Existing domestic laws covering cyber-enabled crimes and means of establishing jurisdiction over them vary widely across the globe. This **divergence may lead to jurisdictional disputes**, undermine predictability and trust, and hinder international cooperation on sharing electronic evidence.

To avoid these unintended consequences, we urge states to **maintain strict dual criminality requirements for all crimes and law enforcement measures** covered by this convention. We also encourage states to focus on "*serious crimes*" and require "*criminal intent*" as a prerequisite for exercising any powers over crimes included in this convention. Loose standards such as "*dishonesty*" or "*without a right*" risk criminalizing acts carried out with beneficial intent, such as penetration testing and cybersecurity research. This increases the likelihood of prosecuting individuals for unintentional behavior or behavior that did not cause harm. At a minimum, ethical hackers must be exempted from the scope to protect lawful cybersecurity work that helps keep the digital ecosystem secure. In line with the above, we propose that states:

- **Include "*criminal intent*" as a prerequisite for establishing crimes under this convention**. Less precise standards, such as "*without a right*" or "*dishonestly*", risk involving legitimate users whose accounts may have been compromised and used for criminal activity without their knowledge. According to the latest Microsoft Digital Defense Report, cybercriminals are increasingly using legitimate infrastructure to operate. For example, malicious emails often originate from compromised sender accounts, who may be unaware that their accounts have been used for cybercriminal activities. To this end we propose the following changes:
    - **Art.6(1):** *"Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed ~~intentionally~~ with criminal intent, the access to the whole or any part of a computer system ~~without right~~."*
    - We propose similar changes, mutatis mutandis, in **Art.2(h), 6(2), 7(1), 7(2), 9(1), 10(1), 11(2), 12(b).**
- **Add the "right to appeal" to other international human rights obligations** listed in Art.21(4) (i.e., right to a fair trial and the rights of defense) to align the text with Art.14 & 15 of International Covenant on Civil and Political Rights.
- **Protect data custodians acting in good faith.** States should exempt data custodians from liability for acts undertaken in performance of duties imposed on them by this convention. The convention should prevent scenarios where data custodians face sanctions in one jurisdiction for complying with data request in another. To this end we propose reinserting the following paragraph in Art.18:
    - *"Legal persons shall be protected from liability for an act done or omitted to be done in good faith: (a) in the performance or intended performance of a duty imposed by or under this convention; or (b) in the exercise or intended exercise of a function or power conferred by or under this convention."*

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Chapter III. – Jurisdiction

To effectively combat cybercrime, the convention must **provide clear guidance on which jurisdiction applies** in investigating and prosecuting it. States should avoid adopting an instrument that could inadvertently give rise to jurisdictional disputes, hindering international cooperation. The convention should also not allow for expansive claims of extraterritorial jurisdiction. Otherwise, the convention could create serious conflicts of law problems for data custodians, who may be compelled to violate the law in one jurisdiction to comply with data request in another.

We have previously warned that **offering services in a given country should not provide sufficient grounds for that state to establish jurisdiction** and request data on suspected crimes committed elsewhere. This could lead to data being requested directly from data custodians via procedural and law enforcement powers, including through real-time surveillance. Such scenarios raise serious human rights concerns and could undermine national security, particularly if data custodians are not allowed to notify impacted individuals and states where those individuals reside.

Unfortunately, the zero draft currently allows for such situations to occur. As proposed, Article 22 **only provides guidance on establishing jurisdiction over crimes defined in the convention** (i.e., those included in Art. 6 to 16). This leaves states with wide discretion to decide how to establish jurisdiction over other "*crimes committed by a means of a computer systems*" for the purposes of exercising their powers under procedural measures and international cooperation measures. As a result, the potential for jurisdictional disputes is severe.

Microsoft has stressed that when conducting extraterritorial surveillance, governments must comply with their international legal obligations, including the principles of sovereignty and non-intervention. States **must not use extraterritorial measures to circumvent other legal mechanisms,** such as mutual legal assistance treaties to obtain data located outside their territory directly from data custodians who offer services in multiple jurisdictions. In line with the above, we propose that states:

- **Limit the scope of all procedural and international cooperation measures only to crimes defined** in this convention (see our proposed amendments for chapters I., IV., and V.).
- **Align Art.22(5) with the text of with the text of the Budapest Convention** to place emphasis on "*determining the most appropriate jurisdiction for prosecution*" rather than on "*coordinating actions*".
- **Ensure that offering services in a given country is not used as the sole basis to establish jurisdiction** and request data from data custodians by amending Art.22(6) as follows:
    - *"Without prejudice to norms of general international law, this Convention shall not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law save that jurisdiction shall not be based solely on whether nationals of one State Party use services offered by a data custodian located in another State Party".*

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Chapter IV. – Procedural Measures

Microsoft has called on states to include robust safeguards throughout the convention to protect people from potential abuse of executive authority. We also urged states to **limit the scope of application of all procedural measures** to precisely defined crimes set forth in this convention. A narrow scope is necessary to ensure that technology industry and data custodians have a clear understanding of what constitutes a cybercrime so that they can respond appropriately to government requests for information.

Unfortunately, the chapter on procedural measures, as currently drafted, resembles a **global data access treaty rather than an instrument designed to curb cybercrime**. It includes expansive provisions for government access to personal data, including intrusive measures for real-time surveillance, granting governments wide discretion to request data on a plethora of cyber-enabled crimes not defined in this convention. Combined with the lack of clarity on jurisdiction for this category of crimes, data custodians will have no way of determining whether government requests for data access are reasonably tied to the state's jurisdiction (unless electronic evidence is requested for crimes defined in Art. 6 to 16). Furthermore, the draft text contains no transparency safeguards that would allow data custodians to notify the target of surveillance or even the country in which the target resides, of the ongoing investigation.

Such broad scope introduces dangerous levels of uncertainty and will frustrate international cooperation. Without robust safeguards, the intrusive digital surveillance measures envisioned under this draft convention could unfold in total secrecy, undermining both human rights and national security. This broad expansion of digital surveillance powers will also **clash with existing human rights obligations and data protection standards**. This will likely erode trust, produce jurisdictional disputes, and ultimately undermine global efforts to combat cybercrime. In line with the above, we propose that states:

- **Limit the scope of application of procedural measures to a precisely defined set of crimes** included in the criminalization chapter to avoid uncertainty for prosecutors and data custodians operating across countries. To that end, we propose the following changes:
    - **Deletion of section (b) of Art.23(2) in its entirety.**
    - **Art.23(2)(c)**: *"The collection of evidence in electronic form of offences set forth in this convention ~~any criminal offence~~."*
    - **Art.27(1):** *"Subject to the other provisions of this Convention, including Article 5 and Article 24, ~~E~~each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, where there is reasonable belief that a criminal offence set forth in this Convention was committed or is being committed, and where the State Party in question can reasonably claim jurisdiction over such offense, to ~~order~~ request:"*
    - We further recommend implementing similar changes, mutatis mutandis, in Art. 28(1).
- **Ensure the purpose and reach of government access to data remains narrowly tailored** to meet specific public safety and national security needs. We reiterate that real-time collection of data can lead to a significant invasion of privacy and believe that without robust safeguards and independent judicial authorization, provisions on real-time collection of data would contravene the principles of necessity and proportionality.

  Furthermore, traffic data refers to records of communication consisting of indicators such as start and stop time, origination point (calling number, FROM address), and destination point (called number, TO address). As such, it is an after-the-fact record of communication or activity that is not collected by data custodians in "*real-time*". We recommend that states address the issue of traffic data via a "*retention*"

approach rather than via provisions on "real-time collection", which is conceptually flawed and technically not feasible. For those reasons, we propose:

- **Deletion of Articles 29 and 30 on real-time collection of electronic evidence** and, mutatis mutandis, corresponding provisions, such as those included in Art.23(3).
- **Add Art.24(6): "***Each State Party shall ensure that computer data acquired by it pursuant to the powers and procedures of this Convention are not used for purposes other than those for which it was originally requested."*

- **Establish a clear line of responsibility for responding to government data access requests** from law enforcement agencies to data custodians. Currently, Article 28(4) makes it possible for states to order "*any person who has special knowledge*" of a particular computer system to provide the necessary information to search that computer system. In the absence of independent oversight and due process safeguards, such provision runs the risk of being abused to compel, for example, an engineer or a company employee with special knowledge of an ICT system to provide assistance in subverting technical access controls such as access credentials, encryption, and just-in-time approvals, thereby allowing data exfiltration without the knowledge of the responsible data custodian. Such provision could not only expose individual employees of IT companies to coercion and criminal prosecution but could also undermine cybersecurity of ICT products and services more broadly. Instead, we urge states to ensure that the convention ensures that the data custodian (i.e. a legal person) and its executive officers are responsible for processing data access requests. For those reasons, we propose:
  - **Deletion of Article 28(4) in its entirety.**
- **Introduce meaningful human rights safeguards** to protect people from potential abuse of executive authority. Except in narrow circumstances, the public has a right to know how, when, and why governments seek access to their data. States need to ensure transparency and accountability in the conduct of law enforcement authorities including by proving notice to impacted individuals. Secrecy should be the exception rather than the rule. With that in mind we propose states:
  - **Preserve the right of data custodians to challenge government demands** for data on behalf of users, including based on potential conflicts of law.
    - **Add Art.24(2)(i):** "*[This shall include:] the ability of third parties to challenge requests made by a State Party in relation to the powers and procedures of this Convention on the basis of legality, proportionality, or necessity, with such challenges to be adjudicated by an organ of the State Party independent of the requesting agency*;"
    - **Add the following sentence to Art.24(3): "***This shall include ensuring that liability does not arise for third parties that do not act as requested or required by a State Party in relation to the powers and procedures in this Convention where doing so would require it, or them, to act unlawfully in the jurisdiction of another territory*."
    - **Add new Art.28(4):** *"States Parties shall ensure that custodians are permitted to challenge requests made under Article 28."*
  - **Tie government data requests to independent judicial authorization**. Law enforcement demands for content and other sensitive user data should be reviewed and approved by an independent judicial authority prior to enforcement of the order, and only after a meaningful minimum legal and factual showing.

- **Add Art.24(2)(ii):** *"the ability of third parties to initiate a review of decisions made in relation to Article 24.2(i) independent of the organ of the State responsible for adjudicating the decision;"*

- **Protect users' human rights, including the privacy of their data** and secure a right to redress for any individual and entities whose rights were violated through the exercise of powers set forth in this convention.

  - **Duplicate Art.37(8) as Art.24(4) to ensure safeguards apply horizontally: "***Nothing in this Convention shall be interpreted as imposing an obligation to cooperate if the requested party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin, membership of a particular social group, or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons, or if there are substantial grounds for believing that the person would be in danger of being subjected to politically motivated persecution, torture, or inhuman and degrading treatment or punishment."*

  - **Add Art.24(5):** *"Each State Party shall ensure that the computer data, including traffic data, of persons who are subject to the jurisdiction of another State Party or territory, which is acquired by the State Party through the powers and procedures of this Convention, are protected from disclosure to unauthorized persons, or modification, and shall delete any such data held expeditiously when it is no longer required for an ongoing investigation or prosecution."*

- **Preserve the right for data custodians to give users notice**, especially where doing so does not interfere with or otherwise compromise an ongoing investigation or prosecution. Microsoft believes that except in narrow circumstances, the public has a right to know how, when, and why governments seek access to their data. With that in mind we recommend:

  - **Add Art.24(2)(iii):** *"the ability of third parties who are custodians of computer data to notify legal or natural persons when a State Party requests the disclosure of their computer data, including traffic data, provided that doing so does not endanger an ongoing investigation, prosecution or proceedings, and to publish the number of requests they receive from each Stat Party on a periodic basis."*

  - **Amend Art.25(3):** *"Each State Party shall adopt such legislative and other measures as may be necessary, subject to conditions outlined in Article 27, to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for a period of time, but no longer than necessary to serve law enforcement's demonstrated need for secrecy."*

  - **Add Art.27(2):** *"The convention recognizes that absent narrow circumstances, users have a right to know a State Party requires a data custodian to submit information and, unless secrecy is required as outlined in Article 27(3), data custodians shall have a right to notify users."*

  - **Add Art.27(3):** *"When confidentiality is required, the competent authorities shall be required to (1) make their case for secrecy to an independent authority, such as a judge; and (2) present case-specific facts to justify both why the State Party should not be obligated to notify the target and why the State Party must limit the data custodian's right to notify its customers of the request. Any nondisclosure order imposed on a data*

custodian must be narrowly limited in duration and scope and must not constrain the custodian's right to speak any more than is necessary to serve a demonstrated need for secrecy. Data custodian must also be permitted to challenge these requests to ensure that government nondisclosure orders satisfy these requirements."

- **Ensure that key provisions do not defer extensively to domestic law and include transparent data minimization, retention, and dissemination limits**. In our experience, conflicting rules raise barriers to effective cooperation. Microsoft frequently deals with situations where one country's laws conflict with lawful demands from another country, which is often a lengthy, costly, and difficult process. Global efforts to fight cybercrime will be significantly enhanced if the convention harmonizes rules across jurisdictions and ensures synergies with existing international obligations and instruments. In particular, the convention should not be used to indefinitely extend retention periods by deferring to domestic laws. It should provide a specific limit and, in our view, preservation for up to a maximum of ninety days to enable the competent authorities to seek data disclosure, is the most appropriate. In line with these comments, we propose the following changes:
  - **Art.25(2): "***A State Party may provide for such an order to be subsequently renewed for one further period of ninety days only and must supply reasons for such an extension."*
  - **Art.26(1)(a):** *"~~Ensure~~ To the extent technically possible and subject to domestic legislation, enable that such expeditious preservation of traffic data is available for a period of ninety days, renewable for another period of ninety days regardless of whether one or more ~~service providers~~ data custodians were involved in the transmission of that communication."*
  - **Art.*42(8):*** *"Before the expiry of the preservation limit in paragraph 7, the requesting State Party may request an extension of the period of preservation, for not more than ninety additional days. If the requesting State Party does not submit a request for the disclosure of the data at the expiry of 60 days, then the requested State Party shall direct the data custodian to delete the data."*

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Chapter V. – International Cooperation

The primary purpose of the convention should be to encourage effective international cooperation between and among national law enforcement and prosecutorial agencies in investigating and prosecuting cybercrime. It should complement existing networks and mechanisms, draw on effective treaties and measures, respect due process principles. The convention should also **minimize conflicts with existing laws and create mechanisms to resolve any disputes that arise**.

With that in mind, Microsoft urges states to ensure that international cooperation provisions apply to a precise and narrowly defined set of crimes specified in this convention, and which can be commonly understood across jurisdictions to satisfy dual criminality criteria. These provisions should also focus on actions conducted with criminal intent that are punishable by at least four years of imprisonment (i.e. serious crimes). **Without clear scoping, the convention could undermine existing international cooperation** by overwhelming law enforcement agencies, private sector entities, and data custodians with information requests for minor offenses that may not be commonly understood as crimes across jurisdictions. This could also gravely impact basic human rights such as privacy and freedom of expression and undermine the work of cybersecurity experts and researchers.

To avoid these undesired outcomes, the provisions on international cooperation should apply only to crimes defined in the criminalization chapter. This chapter should also **include actionable provisions on transparency, refusal on the grounds of absence of dual criminality** or political offences (if cyber-enabled crimes are included), and in instances where individuals may be prosecuted on grounds of their race, religion, gender, or other internationally protected characteristics. The provisions in this chapter should also ensure that human rights protections and due process safeguards are explicitly factored in at every step of the process. In particular, the rights to free expression, access to information and privacy – as enshrined in existing international human rights instruments – must be protected in line with the required minimum standards of legality, proportionality, and necessity. In line with the above, we recommend states:

- **Limit the applicability of international cooperation provisions to a precisely defined and commonly understood set of "serious" crimes**. The chapter on international cooperation currently extends the scope of application of all cooperation measures to all "*serious crimes*". As emphasized previously, domestic definitions of such crimes vary widely across jurisdictions and will increase uncertainty in this space. We therefore propose the following changes:
    - **Art.35(1) and mutatis mutandis in Art.40(1) :** *"States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters, and domestic laws, for the purpose of investigations, prosecutions and judicial proceedings concerning serious offences established in accordance with articles 6 to 16 of this Convention, or for the collection, obtaining, preservation and sharing of evidence in electronic form of serious offences established in accordance with articles 6 to 16 of this Convention~~, as well as of serious crime, including those offences covered by article 17 of this Convention when applicable~~."*
    - **Align Art.37(1) on extradition with the definition of serious crime** provided for in the Use of Terms section by limiting extradition to serious offences "*punishable by a ~~maximum~~ minimum deprivation of liberty of at least ~~one~~ four years*". We presume the word "*maximum*" currently included in the text is an error.
        - **Delete last part of Art.47(1)(a):** *"[State Parties shall take measures] To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services in order to facilitate the secure and rapid exchange of*

information concerning all aspects of the offences covered by this Convention, ~~including, if the States Parties concerned deem it appropriate, links with other criminal activities~~;"

- **Establish dual criminality as a key prerequisite for international cooperation**. Microsoft has previously emphasized that data custodians, technology industry included, will need to have a clear and shared understanding of what constitutes a cybercrime to be able to respond appropriately to government requests for information. Without harmonization, conflicts of law may arise, making effective cooperation and timely information-sharing impossible. The current Article 35(2) does not establish clear and predictable dual criminality requirements. At a minimum, offences triggering international cooperation should (a) exist within the same or similar category of a crime, (b) be punishable by a deprivation of liberty of at least four years and (c) represent at least one of the crimes defined in Articles 6 to 16 in the criminalization chapter. We therefore propose states:
    - **Amend Art.35(2):** "*In matters of international cooperation, ~~whenever~~ dual criminality ~~is~~ shall be considered a necessary requirement, and ~~it~~ shall be deemed fulfilled ~~irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as that of the requesting State Party, or~~ if the ~~conduct of the underlying~~ offence for which assistance is sought is a serious criminal offence established in accordance with articles 6 to 16 of this Convention in both the requesting and the requested State*."
    - **Add Art.43(3):** *"A State Party that requires dual criminality as a condition for responding to a request for mutual assistance in the search or similar accessing, seizure or similar securing, or disclosure of preserved traffic data may refuse the request for preservation under this article in cases where it has reasons to believe that, at the time of disclosure, the condition of dual criminality could not be fulfilled."*
- **Incorporate robust safeguards and grounds for refusal throughout the international cooperation chapter.** The chapter, should, at a minimum, include actionable safeguards related to transparency, data protection, and grounds for refusal in instances where individuals may be persecuted on account of their race, religion, gender, or other internationally protected characteristics. In particular, Article 24 on safeguards should apply to all relevant measures in this chapter. We propose the following changes:
    - **Delete articles 45 and 46 on mutual legal assistance in the real-time collection of traffic and content data in their entirety.** We reiterate that real-time collection of data can lead to a significant invasion of privacy and believe that without robust safeguards and independent judicial authorization, provisions on real-time collection of data would contravene the principles of necessity and proportionality. We recommend that states address the issue of data via a "*retention*" approach rather than via provisions on "*real-time collection*".
    - **Add. Art35(3):** *"The powers and procedures provided for in this chapter shall be subject to the conditions and safeguards provided for in article 5 and article 24."*
    - **Amend Art.40(21)(a) and mutatis mutandis Art.42(5) and Art.43(2):** *"[Mutual legal assistance may be refused] if the request is not made in conformity with the provisions of this article or article 24 of this convention."*
    - **Add Art.40(21)(b)bis:** *"[Mutual legal assistance may be refused] if the requested State Party concludes that the execution of the request would likely violate fundamental human rights of the accused person."*

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

- **Add Art.44(4):** *"Disclosure of stored computer data under paragraph 1 may be refused on the basis of the grounds contained in article 40(21) and article 24."*
- **Add Art. 36(5):** *"This article is without prejudice to States Parties' domestic legal framework where it imposes conditions on the transfer of personal data to other States."*
- **Amend Art.37(8):** *"Extradition shall be subject to the conditions and safeguards provided for in paragraph 15 of this article as well as by the domestic law of the requested State Party ~~or~~ and by applicable extradition treaties […]."*
- **Delete the phrase "*other persons concerned*" in Art.46(1)(b-i)** as it is unclear why states should be obliged to disclose information on location and activities of persons not suspected of having committed offences covered under this convention.
- **Subject extradition to a clear set of conditions and safeguards**. At a minimum, Article 37(9) should encourage states to "*harmonize*" expectations around the sufficient evidentiary basis required for extradition, rather than call on states to *"simplify evidentiary requirements"*. Furthermore, to strengthen extradition safeguards we propose to explicitly tie the conditions for extradition included in Article 37(8) to safeguards enumerated in Article 37(15) and to align paragraph 15:
  - *"Extradition shall be subject to the conditions and safeguards provided for in paragraph 15 of this article as well as by the domestic law of the requested State Party ~~or~~ and by applicable extradition treaties, including, inter alia, the grounds upon which the requested State Party may refuse extradition."*
- **Incorporate transparency as a rule.** In line with our proposals to preserve the right for data custodians to give users notice in the chapter on procedural measures we propose the following changes in this section:
  - **Add Art.36(4):** *"Where the source of the data requested is a third-party custodian of the data that custodian may notify the data subjects when a State Party requests the disclosure of their computer data, including traffic data, provided that doing so does not prejudice an ongoing investigation, and may publish the number of requests they receive from each State Party on a periodic basis."*
  - **Add Art. 40(19bis):** *"The requested State Party shall, unless confidentiality is required as outlined in article 27(3) of the present convention, notify the accused person."*
  - **Amend Art.40(20):** *"When confidentiality is required as outlined in Article 27(3), the requesting State Party may require that the requested State Party keep confidential, for a defined period of time, the fact and substance of the request, except to the extent necessary to execute the request. Such request should be made in writing and include detailed explanation as to why confidentiality is necessary so as not to endanger an ongoing investigation, prosecution or other proceeding. If the requested State Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting State Party."*
  - **Amend Art.42(2)(g):** *"[A request for preservation shall specify] ~~As appropriate,~~ If there is ~~the~~ a need to keep the request for preservation confidential and not to notify the user, the rationale for confidentiality congruent with Article 27(3) of this Convention."*

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

- **Strengthen personal data protection** to ensure that states' data protection frameworks are not overridden by this convention and that end users are adequately protected against potential misuse or unauthorized dissemination of their data. Importantly, when discussing personal data protection, the convention should ensure states transmitting personal data do so in accordance with established international principles and agreements. To that end we propose the following change:
    - **Add Art.36(5):** *"This article is without prejudice to States Parties' domestic legal framework where it imposes conditions on the transfer of personal data to other States."*
- **Fully align international cooperation provisions with existing international human rights instruments.** As a general principle, we would encourage states to ensure that this convention does not quote selectively from existing instruments or alter the quotes. By way of example, the extradition exemption included in article 37(15) mirrors existing international instruments, including the International Refugee Convention only partially and selectively.
    - We therefore urge states to reinsert the phrase "*membership of a particular social group*" to fully align **article 37(15**) with article 33 of the Refugee Convention. Additionally, we also recommend adding the phrase "*politically motivated persecution, or inhuman and degrading treatment or punishment*" next to the existing reference on torture in that same article to cover all relevant provisions of the Convention against Torture.
    - **Add Art. 40(3bis):** *"The provisions of this article shall not affect the obligations under existing human rights instruments, nor any other treaty, bilateral or multilateral, that governs or will govern, in whole or in part, mutual legal assistance."*
    - **Add references to "*existing international obligations*"** in zero draft provisions that defer to domestic laws, including in, but not limited to, draft articles 37(8)(9)(10)(13), 40(6), 40(21)(c), 42(3), and 47(1).
    - **Add references to existing "*international human rights obligations*"** or "*applicable human rights instruments*" in relevant sections of the draft that currently inappropriately defers exclusively to domestic laws, including in draft articles 37(14), 40, and 55.
- **Mainstream the principles of legality, necessity, and proportionality** in relevant provisions throughout this convention, including but not limited to:
    - ***Art.40(30)(b):*** *"[The requested State Party] may, at its discretion, provide to the requesting State Party, in whole, in part or subject to such conditions as it deems appropriate, copies of any government records, documents or information in its possession that under its domestic law are not available to the general public, provided that such records or documents are relevant to the investigation, prosecution or proceeding in question and meet the criteria of proportionality, necessity, and legality."*
    - ***Art.47(1)(i):*** *"The identity, whereabouts and relevant activities of persons suspected of involvement in such offences ~~or the location of other persons concerned~~".*
    - ***Art.*24(1):** *"Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards provided for under its domestic law, which shall be consistent with its obligations under international human rights law, and which shall incorporate the principles of proportionality, necessity, and legality."*

- **Clamp down on "safe havens" for cybercriminals.** Even the most streamlined procedures for exchanging electronic evidence and obtaining data access will not achieve their desired results if cybercriminals continue to leverage safe havens to evade prosecution and accountability. Where there is an indictment supported by evidence acquired through legal process, subject to the protections outlined above, individuals engaged in cybercrime should be subject to formal extradition proceedings. In this context, we commend preambular paragraph 5 which highlights the determination of states to "*deny safe heavens to cybercriminals*" and article 56(4) proposing to address this issue through technical assistance. However, to address the challenge of safe havens more comprehensively, we also recommend the following:
    - **Amend Art.37(20)**: *"States Parties shall seek to conclude bilateral and multilateral agreements or arrangements to carry out or enhance the effectiveness of extradition and to take other appropriate measures against States who harbor cybercriminals within their jurisdictions."*
    - **Revise Art.40(21)(b)** by removing "*other essential interests*" from the list of reasons for legitimate refusal for mutual legal assistance. As currently drafted, we fear this provision is too broad and could potentially be used by states as an excuse not to extradite cybercriminals hiding within their jurisdictions.
- **Protect the targets and victims of cybercrime, including by offering them effective remedies**. We welcome the inclusion of article 52 on the recovery and return of proceeds of cybercrime and we call on states to enable victims to initiate civil action in courts of other states to protect their property rights violated by cybercriminals. With that in mind, we propose the following changes:
    - **Art.52(1):** *"Proceeds of crime or property confiscated by a State Party pursuant to article 31 or 50 of this Convention shall be disposed of by that State Party including by returning it to its prior legitimate owners whenever possible, and in accordance with its domestic law and administrative procedures."*
    - **Art 52(2): "***When acting on a request made by another State Party in accordance with article 50 of this Convention, States Parties shall~~, to the extent permitted by domestic law and if so requested,~~ give priority consideration to returning the confiscated proceeds of crime or property to the requesting State Party so that it can give compensation to the victims of the crime or return such proceeds of crime or property to their prior legitimate owners."*

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Chapter VI. – Preventive measures

Microsoft recognizes the importance of preventive measures in fighting cybercrime, including cybersecurity education, capacity building, awareness raising, and increased public-private cooperation. The **implementation of technical measures, such as encryption or multifactor authentication** is similarly pivotal. These investments make the online environment safer, raising the barrier to entry for cybercriminals.

However, we believe that the convention should primarily focus on addressing cybercrime and prosecuting cybercriminals. Its **scope should not be expanded to include cybersecurity measures** or increasing the overall societal resilience in cyberspace. Other instruments are available to address those areas and the convention should focus on public authorities rather than introducing industry regulation. States have typically focused on developing frameworks and legislative approaches to increase cybersecurity and cyber resilience in non-criminal contexts, and we commend the zero draft for maintaining this separation.

We further **commend the references to anonymous reporting of ICT incidents contained in Article 53(4)**. We have repeatedly called for the convention to protect security researchers, ethical hackers, and penetration testers, as they perform essential work in improving the security of the digital ecosystem. Individuals engaged in lawful cybersecurity work should be exempt from the scope. The reference to anonymous reporting of incidents should be expanded to also cover ICT vulnerabilities and the following exemption included in the chapter on general provisions:

- **Add Art.3(3) to protect ethical hackers and cybersecurity researchers:** "*This Convention shall not apply to acts conducted in good faith undertaken to reduce the potential for harmful interference with computer systems or computer data, including traffic data, associated with such systems or to improve their resilience.*"

We would further recommend **replacing the term "immediate" with "expedited" in Art.53(3)(g).** We note that the immediate removal of child sexual abuse and exploitation material may not always be possible, particularly if digital evidence is to be first sealed for potential use in court.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Chapter VII. – Technical assistance and capacity building

Cybercrime knows no borders, and an effective response to it must enable states, civil society and the private sector to effectively work together. However, states are currently at vastly different levels of readiness when it comes to cybercrime investigation and prosecution**. Capacity building is needed to empower both public authorities**, and the rest of multistakeholder community.

Microsoft welcomes provisions in this chapter that create a framework for training programs, as well as technical assistance to support the implementation of the convention. In this context, we recall existing cybersecurity capacity building principles, agreed through the adoption of the 2021 consensus report of the Open-ended working group on cybersecurity (A/75/816). These principles state that **capacity building should respect human rights and fundamental freedoms**, be gender sensitive, sustainable, results-focused, demand-driven, voluntary, and tailored to specific needs and contexts. Microsoft believes that these principles, endorsed by the General Assembly, should be reflected in this chapter and guide its provisions. In line with the above, we recommend that states:

- **Incorporate existing cybersecurity capacity building principles into the convention** through a direct reference to the OEWG 2021 consensus report and align individual provisions in this chapter with specific principles on (a) processes, (b) partnerships, and (c) people contained in paragraph 55 of the said report, including by:
    - **Adding Art.56(7): "***States Parties and other implementing organizations shall ensure that the assistance efforts undertaken in support of capacity-building are subject to appropriate and transparent monitoring and evaluation processes to assess their effectiveness and compliance with existing international obligations, human rights in particular.*"
    - Highlighting the voluntary nature of cooperation, including in Art.54(6), Art. 55(2), and 56(2)(d).
- **Recognize the expertise non-governmental stakeholders can bring into capacity building work**, including through their contributions to information sharing, training programs and technical assistance. To that end, we propose the following:
    - **Amend Art.54(2) and, mutatis mutandis, 54(5):** "*States Parties shall, to the extent necessary, initiate, develop, implement or improve, in voluntary collaboration with stakeholders whenever appropriate, specific training programs for their personnel responsible for the prevention, detection, investigation and prosecution of the offences covered by this Convention*."
    - **Amend Art.55(2):** *"The States Parties shall, on a voluntary basis, consider developing and sharing with each other, and with stakeholders, ~~and through~~ international and regional organizations statistics, analytical expertise and information concerning cybercrime with a view to developing, insofar as possible, common definitions, standards and methodologies, including best practices to prevent and combat such offences."*
- **Expand the envisioned training programs in Art.54(3) by two common problem areas** that in our experience often delay or frustrate cooperation and prosecution of cybercrime:
    - *"Methods for addressing, and training to address, conflicts of laws arising where requests made by one State Party to another would require a third party to infringe the law in one of the concerned State Parties."*
    - *"Methods for addressing, and training to address, common issues in the formulation of requests for cooperation between States Parties that are refused because the request is overly broad or not sufficiently specific.*

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Chapter VIII. – Mechanisms of implementation

Microsoft recognizes that for the convention to deliver impactful outcomes, its provisions must be more than just words on paper. It is essential to **create and empower effective mechanisms of implementation**. We call on states to draw on existing mechanisms that have proven successful.

We believe that a treaty body, such as a Conference of the Parties or Meeting of the Parties, should oversee the operation and effectiveness of the convention, as currently proposed. Given the role of technology industry in this space, it would be appropriate for the convention to **explicitly affirm a meaningful role for ICT companies in these meetings**. Previous experience from regional bodies, such as the Council of Europe's Cybercrime Committee, has shown the value of public private cooperation in this area.

We have also previously emphasized that any follow-up convenings to improve capacity and collaboration to counter cybercrime within the framework of this convention should include technical experts from the ICT industry and the broader multistakeholder community. This could be achieved by:

- **Adding the text of the current AHC modality on stakeholder participation in article 57**. This stakeholder modality, approved by consensus in the relevant UN General Assembly resolution (A/RES/75/282), gives non-ECOSOC organizations, including industry, the opportunity to meaningfully participate in UN cybercrime treaty negotiations, whilst protecting the decision-making prerogatives of states. Embedding this modality firmly in a future mechanism of implementation would ensure that states can continue to benefit from the expertise of the multistakeholder community.
- **Strengthening the reference to stakeholder input** in article 57(6) to read as follows: "*Inputs received from relevant non-governmental organizations ~~duly accredited in accordance with procedures to be decided upon by the Conference of the States Parties~~ ~~may~~ will also be considered.*"
- **Creating an expert forum** that would allow states, industry, and the broader technical community to exchange views on the latest cybercrime threats and potential mitigation measures. Given the dynamic nature of cybercrime, such a forum would greatly enhance public authorities' ability to respond effectively and timely to evolving threats.