Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Cybercrime Convention Negotiations

Microsoft's submission to the Seventh 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. There is no question that a more effective international cooperation framework against cybercriminal activity would be beneficial. As we all know, cybercrime remains a growing problem, set to cost the world trillions of dollars each year. Therefore, the intended purpose of a new UN Convention on Cybercrime should be to aid the international community to fight the scourge of cybercrime.

However, Microsoft remains gravely concerned with the revised draft. We are disappointed that our key concerns, that we and other industry and civil society entities broadly and continuously shared with member states, have not been addressed in the revised text. In fact, several of the already harmful provisions are now broader and several limitations on the scope have been removed, making the revised text significantly worse than previous versions.

In line with our previous submissions, we believe the success of these negotiations and the effectiveness of the resulting Convention depend on a narrowly defined scope and consensus-based agreement. The new Convention should therefore apply only to serious offences defined in the text and should focus on addressing cyber-dependent crimes.

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, we urge the AHC to rely on high level cooperation principles, rather than detailed procedural cross border provisions, which will inevitably give rise to conflicts of laws for Service Providers. Cooperation must be based on predictability and trust. It can only be achieved if the offences and powers set forth in the Convention are commonly understood and applied transparently by all parties involved. As we have repeatedly stated, 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.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

We urge states to spend the final session crafting a Convention that fulfils its intended purpose: To aid the international community in fighting cybercrime rather than one that creates an environment for cybercrime to thrive and makes cyberspace considerably less secure. In its current form, this treaty will erode data privacy, threaten digital sovereignty, and undermine online rights and freedoms globally. We could not recommend any state sign or ratify a Convention with such profound negative impacts on the digital ecosystem.

Against this background, we provide the suggestions below in addition to our previous language especially from the 5th and 6th sessions.

As a matter of priority, we believe states should:

1) **Clearly and narrowly define the scope of this Convention:** We have continuously called for a narrow and clear scope of this Convention. However, the latest draft text significantly expands the scope so that it is no longer tied to specific crimes previously outlined in articles 6-16, but to a wide range of criminal activities that use information and communications technology. We urge states to reinsert "in accordance with articles 6 through 16," language throughout the draft Convention. Otherwise, this broad definition moves the Convention far away from its original intent, to combat cybercrime and encompasses criminal activity far outside the scope of what should be included.
2) **Improve safeguards throughout the Convention, specifically as it pertains to covert surveillance:** The inclusion of "service provider established or located," in each territory permits joint state action for covert surveillance on individuals in third states, raising concerns about extraterritorial surveillance occurring in total secrecy and without any safeguards. This directly impacts the privacy and rights of individuals and immediately creates conflicts of law and threatens digital sovereignty. We urge states to include robust safeguards throughout the convention and grounds for refusal in the chapter on international cooperation.
3) **Strengthen protections for cybercrime victims and witnesses:** Provisions for victims and witnesses were previously weak, but the new draft makes these protections optional, leaving vulnerable individuals impacted by cybercriminals reliant on varying and potentially inadequate domestic legislation in each country. States must strengthen safeguards for victims and witnesses of cybercrime activity.
4) **Remove new provision on the criminalization of "deception":** The inclusion of a new provision criminalizing any "deception" that alters behavior is overly and dangerously broad. The lack of a precise definition of "deception" allows each state to interpret this provision independently. This ambiguity threatens numerous legitimate online activities to criminal prosecution, undermining the clarity and fairness of the draft Convention.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Detailed comments on revised draft of the UN Convention on countering cybercrime

Our understanding is that the seventh substantive session of the Ad Hoc Committee, in 2024, will focus on the revised text of the Convention with the aim of reaching consensus on the text ahead of the General Assembly 5th in the Fall of 2024. Microsoft's submission responds to key elements contained in each chapter and builds on our previous submissions. For most of the revised text, Microsoft's previous issues from the zero draft were not addressed and we therefore refer to previous submissions from the 5th and 6th sessions.

Scope of the Convention

Clearly and narrowly define the scope of this Convention. Microsoft continues to believe that the Convention's primary purpose should be to encourage effective international cooperation between and among national law enforcement and prosecutorial agencies in investigating and prosecuting cybercrime. As such, the final Convention must **focus on a clear and narrowly defined set of crimes which can be commonly understood across jurisdictions**. Microsoft reiterates that for the Convention to be effective, the technology industry and data custodians must have a clear understanding of what constitutes 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. As we head into the final negotiating sessions, it is both telling and concerning that states have not agreed on the definition of cybercrime, and therefore the scope and intent of the Convention itself. In order to facilitate agreement around the scope, we suggest our proposals on scope included in our submissions from the 5th and 6th sessions in addition to the following:

- *Reinstate "articles 6 to 16" throughout the text as this provides clarity as to what crimes should be criminalized in the Convention (Articles 3.1,18.1,19.1-3, 20, 21.1-7, 22.1, 22.3-4, 23.2a, 31.1 a&b,32, 33.1, 35.1,37.1-3, 38, 39.1,40,41.1, 49, 50.1-2,10, 51.3k).*

Chapter II: Criminalization

Limit the Scope of the Convention. Microsoft again reiterates that terminology must be clear and precise throughout the Convention for it to be an effective tool to help combat cybercrime**.** We urge states to avoid criminalizing broad categories of acts that may be unlawful but not necessarily criminal across jurisdictions, such as "deception." Diverging political, cultural, and legal systems may prevent states from reaching a common understanding of what constitutes "deception of factual circumstances," as the definition of deception is dangerously broad. Including such acts in the scope of this Convention risks overwhelming states and private sector providers with information requests while diverting attention from combating serious cybercrime

offences where prompt action can contribute to disrupting organized cybercrime networks that operate across multiple jurisdictions. Furthermore, existing domestic laws vary widely across the globe and this definition allows each state to interpret this individually and target activities that are protected under many domestic frameworks, such as freedom of expression or privacy. This divergence will likely lead to jurisdictional disputes, undermine predictability and trust, and hinder international cooperation. Therefore, we propose the following:

- *Delete Article 12 (c) in its entirety entirely on deception as the definition is overly and dangerously broad.*

Chapter III: Jurisdiction

Provide clear guidance on which jurisdiction applies in investigating and prosecuting cybercrime. 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. We continue to be gravely concerned about human rights issues throughout this text. In addition to Microsoft's suggestions on this chapter from the 6th session, we propose:

- *Reinstating "articles 6 to 16" in Articles 22.1, 22.3, and 22.4.*

Chapter IV: Procedural Measures and Law Enforcement

Protect individuals' right to privacy and human rights, strengthen personal data protection, and maintain safeguards for victims and witnesses of cybercrime. Individuals should be protected from potential abuse of executive authority, including their right to privacy. Ensuring that personal information is not exploited and remains confidential is paramount to safeguarding individual liberties and fundamental human rights. Furthermore, exploitation of personal information can lead to unwanted surveillance, erosion of personal freedoms and potential abuses of power. Additionally, states' data protection frameworks should not be overridden by this Convention and end users should be 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.

Lastly, one of the key objectives of the Convention should be protecting the targets and victims of cybercrime, including by offering them effective remedies, and setting out an adequate set of

human rights safeguards. The new Convention cannot become an avenue for states to remove or shirk their existing obligations under international law, especially international human rights law. Instead, this Convention should add to or streamline existing international legal obligations with a focus on protecting victims and witnesses.

In addition to the suggestions in our submission for the 6th session, we propose the following:

- *Delete the phrase "content data and subscriber information that has," in Article 25. The collection of content data as included here is concerning as it further a) invades an individual's fundamental right to privacy, b) impacts one's communications – if they are monitored it can have a chilling effect on free speech, c) allows states to discriminate against and target individuals based on certain characteristics such as race, religion, gender or political affiliation, which could disproportionately impact marginalized communities or individuals with dissenting opinions.*
- *Delete the phrase "in accordance with domestic law," in Article 33.1 and delete the phrase, "subject to domestic law, take measures to provide," in Article 34.4. A new cybercrime treaty should further protect victims of and witnesses to cybercrime activity, rather than weaken protections afforded to them. If victims and witnesses know their safety is assured, they are more likely to come forward and report incidents to law enforcement which in turn can allow law enforcement to better investigate and prosecute cybercrimes. The language in the Convention should strive to ensure that victims and witnesses receive consistent protection regardless of where the crime occurred or where they reside rather than being left to often inadequate domestic laws.*

Chapter V - International Cooperation

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. We again reiterate that, except in narrow circumstances, the public has a right to know how, when, and why governments seek access to their data. There is, in our view, a need to ensure transparency and accountability in the conduct of law enforcement authorities and to ensure notice to impacted individuals, provided that this does not compromise an ongoing investigation. Secrecy should be the exception rather than the rule, otherwise users cannot assert their rights and privileges, and trust in both the online ecosystem as well as in the rule of law is undermined.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft remains deeply concerned about this chapter. In addition to our suggested changes in our submission for the 6th session, that unfortunately were not taken into consideration, we propose the following:

- *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".*
- *Delete the phrase "or where data are in the possession or control of a service provider located or established in that other State Party," in Articles 42.1, 44.1, and 45.1 as this introduces conflict of law issues which can create challenges in reconciling legal requirements. For example, if a service provider is subject to the data protection and privacy laws of the country in which it is established, accessing or preserving data will need to comply with those laws. Severe conflict of laws and jurisdictional disputes would arise as a result, reducing trust among states, creating a confusing landscape for service providers to operate in, and fragmenting international efforts to counter cybercrime, ultimately slowing down the ability for law enforcement to cooperate in a cybercrime case.*

In closing, Microsoft reiterates that cybercrime remains a growing problem, set to cost the world trillions of dollars each year. Therefore, the intended purpose of a new UN Convention on Cybercrime should be to aid the international community to fight the scourge of cybercrime. However, to do so it must strike the right balance between security imperatives and fundamental rights, which the revised Convention does not do currently.

Without significant changes, there is a severe risk of creating a digital surveillance treaty in the guise of a cybercrime treaty. In fact, if our key suggestions are not incorporated into a revised text, this Convention will not only gravely harm fundamental rights and create a confusing cooperation landscape for states and providers, but it will allow cybercrime to thrive and make cyberspace considerably less secure.