



15 December 2021

[Redacted]

Ref: OIA-2021/22-0453

Dear [Redacted]

Official Information Act request for responses to the consultation on New Zealand's draft principles and objectives for negotiating a new United Nations convention on cybercrime

Thank you for your Official Information Act 1982 (the Act) request received on 20 October 2021. You requested:

"Can you please provide me with the responses to this recent consultation: <https://consultation.dPMC.govt.nz/un-cybercrime-convention/principlesandobjectives/>"

The timeframe for responding to your request was extended by 20 working days under section 15A of the Act, because consultations had to be undertaken before a decision could be made on the request. Following this extension, I am now in a position to respond.

I have decided to release the requested documents, subject to some information being withheld to protect the privacy of individuals.

In making my decision, I have taken the public interest considerations in section 9(1) of the Act into account.

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on the Department of the Prime Minister and Cabinet's website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Yours sincerely

[Redacted signature]

Tony Lynch
**Deputy Chief Executive
National Security Group**

Submitted to New Zealand's draft principles and objectives for negotiating a new UN convention on cybercrime
Submitted on 2021-10-05 21:58:36

Introduction

1 What is your name?

Name:

s9(2)(a)

2 What is your email address?

Email:

s9(2)(a)

3 Are you answering on behalf of yourself or an organisation? - If organisation, please specify

Organisation:

This is a personal submission

Principles and objectives

4 Do you have any overall views about New Zealand's engagement in negotiations on the cybercrime convention?

Views on NZ's engagement:

In general, I am happy with New Zealand's engagement in negotiations on the cybercrime convention. This is subject to the level and scope of engagement, recognition and inclusion of Māori with the negotiation process.

5 What do you think about the draft principles for New Zealand's engagement in negotiations?

What do you think - principles:

Again, generally supportive New Zealand's engagement in negotiations on the cybercrime convention. This is subject to the level and scope of engagement, recognition and inclusion of Māori with the negotiation process. These principles will obviously be subject to change, how these change in relation to input and inclusion with Māori is critical.

6 Do you have any amendments or additions you'd like to make to the suggested principles for New Zealand's engagement?

Amendments/additions - principles:

In engaging in negotiations, New Zealand will:

- Consider, collaborate and include Māori in the process for providing for Māori interests, the Crown's Treaty of Waitangi relationship, and the potential impact on Māori of issues arising in the negotiation process.

"Seek to encourage and support active Pacific Island Country participation in the negotiations and advocate for their interests where it is necessary, appropriate and required."

Seek to encourage and support active global Indigenous nations participation in the negotiations and advocate for their interests where appropriate.

7 What do you think about the draft New Zealand objectives for negotiations?

What do you think - objectives:

I think it is a robust structure to bring New Zealand to the negotiations. We should use the negotiations as a shield to protect and a sword to cut through barriers.

8 Do you have any amendments or additions you'd like to suggest for the draft objectives?

Amendments/additions - objectives:

- Considers and protects the rights, beliefs, interests of, and potential impact on Māori and indigenous peoples internationally.

9 Are there any particular issues you think are missing from this document?

Anything missing:

Released under the Official Information Act 1982

No, I think it has identified the main items for negotiation. Personally, it is always more satisfying when the cultural aspects of indigenous peoples globally are taken into consideration. When taking this pathway we afford a wider scope to consider.

10 Is there anything else you would like us to consider?

Anything else:

A mechanism to request that those negotiating countries have also afforded their indigenous populations the same level of courtesy as New Zealand.

Next steps

11 Are there particular areas you would like to highlight as key priorities or areas of interest for you in this process?

Areas of interest:

Independent indigenous representation where other nations are able to be supported to have input into the negotiation process.

12 Would you like to discuss any of your feedback or the process more broadly directly by email, phone, VTC, or in person (COVID alert levels permitting)?

No

13 Would you be interested in being consulted again as negotiations unfold? (checking "no" here does not exclude you from future engagement, should you wish to reengage)

Yes

Official Information Act 1982

14 If you think there is a reason why anything in your submission should not be made public, please let us know here.

OIA:

15 If you are an individual, as opposed to an organisation, we will consider removing your personal details from the submission in the event of a request under the OIA. Are you happy for your personal information to be released?

Yes

Released under the Official Information Act 1982

Introduction

1 What is your name?

Name:

s9(2)(a)

2 What is your email address?

Email:

s9(2)(a)

3 Are you answering on behalf of yourself or an organisation? - If organisation, please specify

Organisation:

Global Partners Digital

Principles and objectives

4 Do you have any overall views about New Zealand's engagement in negotiations on the cybercrime convention?

Views on NZ's engagement:

While we remain unconvinced of the need for a new global convention on cybercrime, we recognise that, by virtue of Resolution 74/247, the Ad Hoc Committee on Cybercrime has been mandated to elaborate a comprehensive international Convention on countering the use of information and communications technologies for criminal purposes.

Cybercrime can adversely harm the enjoyment of a range of human rights, including the rights to privacy and to freedom of expression. Appropriate legislation, if effectively and fairly enforced, can help enhance human rights, by protecting people's personal data and information (protecting their right to privacy) and ensuring that electronic communication channels remain open and secure (protecting their right to freedom of expression). The development of appropriate frameworks at the national, regional and global levels to combat cybercrime therefore has significant potential in protecting human rights.

At the same time, however, we have seen across the world how measures taken in the name of combating cybercrime can also pose risks to human rights. Overly broad powers for security and law enforcement agencies to investigate potential criminal offences, for example, or overly broad exceptions to criminal offences which protect individual's rights to privacy, can result in unjustified restrictions on the right to privacy. And where cybercrime frameworks prohibit certain forms of online communications, overly broad criminal offences can constitute unjustified restrictions on the right to freedom of expression.

It is therefore essential that any new framework developed to combat cybercrime at the global level be fully informed by, and consistent with, international human rights law and standards.

5 What do you think about the draft principles for New Zealand's engagement in negotiations?

What do you think - principles:

Overall, we support the principles. However:

While the importance of human rights is recognised in the draft objectives, we believe that the effective protection of human rights should also be a principle underpinning New Zealand's approach. We would suggest adding an additional principle: "Advocate for any eventual convention to be informed by, and consistent with, the international human rights framework, including treaties and their interpretation by authoritative UN bodies."

6 Do you have any amendments or additions you'd like to make to the suggested principles for New Zealand's engagement?

Amendments/additions - principles:

Please see response to question 5.

7 What do you think about the draft New Zealand objectives for negotiations?

What do you think - objectives:

Overall, we support the objectives. However:

- The term “harmful content online” in the third objective should be either removed or clearly and narrowly defined. While there are certainly a small number of types of harmful content where there is an international consensus on the need to address them (in particular child sexual abuse imagery), for many others there is either no universal consensus on how to define the type of content (e.g. “terrorist material” or “extremist material”) or there is no universal consensus that regulatory efforts are needed (e.g. “disinformation”). To ensure that the new convention, and any content-based criminal offences, does not create risks to the right to freedom of expression, it would be helpful if the objectives provided clarity on precisely which types of harmful content should be within scope, and we would urge the government to focus exclusively on those types where there is universal consensus that they need to be addressed through the criminal law and are clearly defined.

- We would suggest greater clarity in the fifth objective as to when it would be appropriate for procedural provisions to apply to offences which do not constitute cybercrimes. Given that many of the measures taken to access electronic evidence are highly intrusive (particularly those that involve surveillance or the collection of communications and other forms of data), a broader discussion would be helpful to take into account broader human rights considerations and to determine what safeguards are needed to ensure that such measures are only used when appropriate and proportionate (for example, only with respect to the most serious offences, only where there is judicial or some other form of authorisation). To reflect this, and to enable that more open discussion, we would recommend rewording the objective as “Recognises that the relevance of digital evidence extends beyond cybercrime and cyber-enabled crime to further offences, and contains provisions relating to appropriate access to electronically stored criminal evidence and the necessary corresponding safeguards.”.

8 Do you have any amendments or additions you'd like to suggest for the draft objectives?

Amendments/additions - objectives:

Please see response to question 7.

9 Are there any particular issues you think are missing from this document?

Anything missing:

Please see responses to questions 5 and 7.

10 Is there anything else you would like us to consider?

Anything else:

We recommend that the development of this convention is based on three key principles:

- First, in order to avoid fragmented approaches, any new convention should build on, and be consistent with, existing frameworks and work undertaken in other parts of the UN, including by the Open-ended Intergovernmental Expert Group Meeting on Cybercrime
- Second, the provisions of the convention should be fully consistent with the international human rights framework, including international human rights instruments and their interpretation by authoritative bodies. Of particular relevance to the convention are the rights to privacy and freedom of expression. In line with well-understood principles of international human rights law, any interference will only be justified if there is a clear and precise legal basis, the interference pursues an objectively legitimate aim, and if it is necessary and proportionate. The convention must ensure that its provisions do not directly or indirectly require or justify interferences with these rights that are not permissible under international human rights law.
- Third, given that cybercrime is an issue affecting a wide range of stakeholders, and that expertise in combating cybercrime exists outside of government actors, it is vital that all relevant stakeholders - including civil society - are able to participate meaningfully in the development of the convention.

Next steps

11 Are there particular areas you would like to highlight as key priorities or areas of interest for you in this process?

Areas of interest:

Our approach towards the development of this convention is based on three key principles.

- First, in order to avoid fragmented approaches, any new convention should build on, and be consistent with, existing frameworks and work undertaken in other parts of the UN, including by the Open-ended Intergovernmental Expert Group Meeting on Cybercrime
- Second, the provisions of the convention should be fully consistent with the international human rights framework, including international human rights instruments and their interpretation by authoritative bodies. Of particular relevance to the convention are the rights to privacy and freedom of expression. In line with well-understood principles of international human rights law, any interference will only be justified if there is a clear and precise legal basis, the interference pursues an objectively legitimate aim, and if it is necessary and proportionate. The convention must ensure that its provisions do not directly or indirectly require or justify interferences with these rights that are not permissible under international human rights law.
- Third, given that cybercrime is an issue affecting a wide range of stakeholders, and that expertise in combating cybercrime exists outside of government actors, it is vital that all relevant stakeholders - including civil society - are able to participate meaningfully in the development of the convention.

12 Would you like to discuss any of your feedback or the process more broadly directly by email, phone, VTC, or in person (COVID alert levels permitting)?

Yes (we will contact you on the email address provided to arrange a further discussion)

13 Would you be interested in being consulted again as negotiations unfold? (checking "no" here does not exclude you from future engagement, should you wish to reengage)

Yes

Official Information Act 1982

14 If you think there is a reason why anything in your submission should not be made public, please let us know here.

OIA:

15 If you are an individual, as opposed to an organisation, we will consider removing your personal details from the submission in the event of a request under the OIA. Are you happy for your personal information to be released?

Yes

Released under the Official Information Act 1982

Submitted to New Zealand's draft principles and objectives for negotiating a new UN convention on cybercrime
Submitted on 2021-10-06 10:40:34

Introduction

1 What is your name?

Name:

s9(2)(a)

2 What is your email address?

Email:

s9(2)(a)

3 Are you answering on behalf of yourself or an organisation? - If organisation, please specify

Organisation:

My organisation

Principles and objectives

4 Do you have any overall views about New Zealand's engagement in negotiations on the cybercrime convention?

Views on NZ's engagement:

It is important for Aotearoa New Zealand to be involved in negotiations and have input into the wording of any convention. Because the Internet works globally to a large extent, it is important that we work with the UN to have a convention working across nations.

Civil society participation is crucial as part of these negotiations, and I refer to the six areas highlighted in this article:

<https://directionsblog.eu/cybercrime-negotiations-affairs-beyond-states/>. Our involvement should make space for and include civil society organisations, and this should be made explicit in the documents. We would like to see a mutually agreed pathway for civil society organisations to participate in this process, both domestically and at the UN, that is properly resourced. Civil society organisations can not participate equitably unless they are resourced to do so.

5 What do you think about the draft principles for New Zealand's engagement in negotiations?

What do you think - principles:

We appreciate the strong wording around our obligations to tangata whenua via Te Tiriti o Waitangi.

The second principle should be a firm commitment to upholding human rights, and the Universal Declaration of Human Rights. It's disappointing that none of the principles explicitly mention human rights, and it is also disappointing to see such a lack in some crucial domestic legislation. Explicit acknowledgement of and commitment to the range of human rights must be included.

While we understand the need to advocate for "our interests", it would be more useful to talk about and think about the interests of all peoples. The perspective of national self-interest can be harmful and hinder good outcomes. While we disagree with the values and approaches of some other governments (particularly where they suppress freedoms and dissent), we can express solidarity with the people of all nations who deserve to live in safety with their rights fulfilled. Therefore, our country's efforts should be consider the interests of all peoples, not just our own.

In focusing on like-minded countries, we need to ensure that this doesn't foster white supremacy or global hegemony of certain nations. Definitions of "like-minded" would be useful, but also an explicit acknowledgement that a diverse range of nations are included in such a definition, so that nations with majority populations of people of colour are afforded equitable power in discussions and negotiations.

Further to this, we would like to see explicit acknowledgement of power dynamics within nations and the effect this has on minority groups. The principles should refer to protections against state overreach (see for example <https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks>), and the need for transparency and accountability of state actors as they deal with cybercrime. While this may create friction with nation states that oppose such transparency and accountability, it will at least make our own position clear and show a commitment from our government to it's own citizens in this regard.

6 Do you have any amendments or additions you'd like to make to the suggested principles for New Zealand's engagement?

Amendments/additions - principles:

See the answer to question 5:

- add explicit acknowledgement of and commitment to the Universal Declaration of Human Rights
- commitment to advocate for the interests of global peoples, not just our own

- explicit commitment to working with a diverse range of countries ie beyond Europe and North America
- protections against state overreach, by use of transparency and accountability mechanisms

7 What do you think about the draft New Zealand objectives for negotiations?

What do you think - objectives:

"Respect for the rule of law" is a concern, as laws in particular nation states can be oppressive and resistance to them might be the most moral position. This should be changed to be changed to respect for all human rights.

There should be an explicit objective on the inclusion of civil society in all discussions and negotiations (refer answer to Question 1).

A "harmonised, modern global framework" - expand this to include the need for agreed definitions that are not over-broad and which will not cap ure legitimate activity.

We support the recognition of Māori and indigenous peoples. A separate point should recognise other marginalised groups, both at global and domestic levels.

8 Do you have any amendments or additions you'd like to suggest for the draft objectives?

Amendments/additions - objectives:

See answer to Question 7, and also:

- a need for an independent oversight body to ensure any convention is being applied fairly by nation states and at a global level. Such a body would also collect evidence on the applications of the convention around who is being impacted and how, effectiveness etc. There may well be existing bodies and processes, but the principles should explicitly mention this and seek to ensure they are fit for purpose and working well.
- need for an effective complaints mechanism to the UN, particularly where nation states are oppressive. Once again, there may already be processes, but this should be explicitly mentioned, as well as ensuring that they are accessible to those who need it most ie those who are vulnerable and marginalised within their own countries.

9 Are there any particular issues you think are missing from this document?

Anything missing:

While there is mention of hate crimes, we would like to see more explicit recognition of incitement to violence, and groups that plan criminal activity - so long as there are adequate human rights protections and that the planning activity has progressed to such a level that there is close proximity to an adverse event.

Cybercrimes should include liability for platforms and providers who knowingly host or publish/disseminate such activities, or who negligently fail to invest in preventative policies and procedures. Once again, any such provisions must have human rights protections, including the protection of the rights of groups to undertake protest and dissent to state oppression.

10 Is there anything else you would like us to consider ?

Anything else:

Next steps

11 Are there particular areas you would like to highlight as key priorities or areas of interest for you in this process?

Areas of interest:

Our particular interest is in online harm cause by hate crimes and hate (or dangerous) speech; dehumanisation of populations; measures to deal with online terrorist content.

12 Would you like to discuss any of your feedback or the process more broadly directly by email, phone, VTC, or in person (COVID alert levels permitting)?

Yes (we will contact you on the email address provided to arrange a further discussion)

13 Would you be interested in being consulted again as negotiations unfold? (checking "no" here does not exclude you from future engagement, should you wish to reengage)

Yes

Official Information Act 1982

14 If you think there is a reason why anything in your submission should not be made public, please let us know here.

OIA:

15 If you are an individual, as opposed to an organisation, we will consider removing your personal details from the submission in the event of a request under the OIA. Are you happy for your personal information to be released?

No

Released under the Official Information Act 1982

7 October 2021

Department of Prime Minister and Cabinet
Parliament Buildings
Wellington

Emailed to: consultation@dpmc.govt.nz

Dear Madam/Sir,

ICNZ submission on the new United Nations convention on cybercrime

Thank you for the opportunity to submit on the new United Nations convention on cybercrime (**the Convention**).

The Insurance Council of New Zealand/Te Kāhui Inihua o Aotearoa (**ICNZ**) represents general insurers and reinsurers that insure about 95 percent of the Aotearoa New Zealand general insurance market, including about a trillion dollars' worth of Aotearoa New Zealand property and liabilities. ICNZ members provide insurance products ranging from those usually purchased by individuals (such as home and contents insurance, travel insurance, motor vehicle insurance) to those purchased by small businesses and larger organisations (such as product and public liability insurance, professional indemnity insurance, cyber insurance, commercial property, and directors and officers insurance).

Please contact s9(2)(a) if you have any questions on our submission or require further information.

Response to questions

Do you have any overall views about New Zealand's engagement in negotiations on the cybercrime convention?

ICNZ supports New Zealand's engagement in negotiations on the cybercrime convention. Unlike traditional crimes, cybercrime operates across borders and can affect many different jurisdictions at one time. It is therefore important for there to be greater understanding of risk and coordination of efforts between countries to improve cyber resilience and minimise the opportunity for cybercrime to take place.

We believe that it is particularly important for a country like New Zealand to take part in the negotiations, as based on engagement with our equivalent organisations in other countries such as Australia, the United Kingdom, France and the United States, New Zealand is still relatively immature in its approach to cyber resilience. It is therefore imperative that we are part of any

discussions about cybercrime and can use it is an opportunity to adopt best practice and learn from other countries where the laws and processes relating to cybercrime are more advanced.

What do you think about the draft principles for New Zealand's engagement in negotiations?

ICNZ believes that the draft principles for New Zealand's engagement in negotiations are appropriate as they align with the values and priorities in the Cyber Security Strategy 2019.

When negotiating, New Zealand should also be mindful of the issues presented by vulnerability. It is possible that there are communities with lower levels of digital literacy and awareness of cybercrime and cyber risk. It is essential that consideration is given to how best to protect these people, and that focus is not solely on businesses and those who are already confident in their use and understanding of devices and internet-based services.

Do you have any amendments or additions you'd like to make to the suggested principles for New Zealand's engagement?

No further suggestions.

What do you think about the draft New Zealand objectives for negotiations?

ICNZ believes that draft objectives for negotiations are largely appropriate, and we particularly support the goal of a harmonised and modern global framework. However, we question whether more of the Cyber Security Strategy priority areas and values could be incorporated into the objectives. For example, resiliency and responsiveness and the protection of national security should also be key considerations when addressing cybercrime.

We also suggest that when referring to "not conflict[ing] with" or "eroding existing instruments", reference is specifically made to the Privacy Act, as our international obligations should be careful not to infringe on the right to protection of personal information.

Do you have any amendments or additions you'd like to suggest for the draft objectives?

We believe that there should also be an objective for greater information sharing between countries in order to facilitate the identification and mitigation of cybercrime risks. Ideally, the Convention will provide for effective and efficient communication about known risks between participants which will raise awareness and allow for mitigation measures to be put in place by those not yet affected.

From an insurance perspective, it is important that as much information about cybercrime as possible is made available. If an insured individual or business were the victim of a cybercrime, it is possible that there would be cover available under a cyber insurance or fidelity and crime policy. To accurately price the risk and to provide resiliency and risk mitigation services, which is now a common part of cyber insurance policies in particular, insurers need to know about size and frequency of incidents occurring in other jurisdictions. Having greater awareness of the risk presented by cybercrime may also allow for improvements to be made to insurance policies or for more cover to be made available.

Are there any particular issues you think are missing from this document?

We do not believe that there is anything missing.

Is there anything else you would like us to consider?

While engaging in negotiations on the Convention, ICNZ believes that it will be critical to consider the differences between state-sponsored and non-state actors, particularly as the risk presented by one group may not reflect that of the other. Both groups will have different motivations as well as varying modus operandi, and for the Convention to be as effective as it can in reducing cybercrime, it will need to consider how to address both state-sponsored and non-state sponsored crime.

Conclusion

Thank you again for the opportunity to submit on the Convention. If you have any questions, please contact our Legal Counsel on s9(2)(a) or by emailing s9(2)(a)

Yours sincerely,

s9(2)(a)



Tim Grafton
Chief Executive

s9(2)(a)



Legal Counsel

Released under the Official Information Act 1982

internet

ABOUT INTERNETNZ

ABOUT THIS SUBMISSION

COMMENTS REGARDING THE PROPOSED CONVENTION

**Helping New Zealanders
harness the power
of the Internet.**

Released under the Official Information Act 1982

As the government mentions in its consultation, “Binding international treaties like the Council of Europe Convention on Cybercrime (the Budapest Convention) have laid the foundations for countries to align their laws and foster information sharing on current threats and best practice.”

We agree. The Budapest Convention, though imperfect, has provided a consistent and predictable framework and we believe that it is important that this framework continues to be both supported and strengthened. We have previously submitted in support of New Zealand’s accession to the Convention.

Ideally, any international discussions on cybercrime would complement the Budapest Convention, as you suggest; however, we are not convinced that this process seeks to do this. On the contrary, we are seeing the possibility where cybercrime is used for a more expansive Internet governance agenda.

On this point, in particular, InternetNZ would like to express our concern about the possibility of this process being used for an “Internet Treaty”.

Over the past few years, we have followed closely the shift in geopolitical power and dynamics and we are aware of the intention of certain countries to see a more top-down, centralized approach to Internet governance. We have grown concerned about the increasing role the United Nations is having in discussions about the future of the Internet.

Of course, we appreciate and support the need for governments to be involved; we have consistently supported the New Zealand government in all its processes. However, we do not necessarily believe that the United Nations is the appropriate venue to discuss such issues due to its non-inclusive structure, which prevents the participation of non-governmental actors. Similarly, we do not believe that a Treaty is necessarily the right choice to address the fast-paced and demanding evolution of the Internet.

This should not be read as endorsing the current Internet Governance framework, which faces a range of challenges and needs reform in several areas. Our current view though is that a United Nations Treaty-led process is not likely to prove the right durable approach to how to manage Internet governance matters.

SPECIFIC REFLECTIONS

Having said all the above, we appreciate that this process is now in motion and that it is important for New Zealand to participate. Below are our reflections on “New Zealand’s Draft Principles and Objectives for Negotiating a new UN Convention on Cybercrime”.

- We are encouraged to see the continuous commitment of the New Zealand government towards “a cyberspace that is safe, secure, stable, multi-stakeholder-governed, free, open and interoperable”. We would like to add to this list the need for an Internet that is globally-connected and has global reach. The global nature of the Internet is a feature not a bug and we need to ensure that it is maintained to the extent possible.
- We also agree with the government’s point that, should this process proceed, it should focus on identifying ways for harmonising some internationally-recognized forms of crime and that it seeks to “address and improve international responses to emergent forms of cybercrime and



cyber-enabled crime”.

- We would like to reiterate the need for this convention to have a narrow and well-scoped purpose. Given the reality and fragile state of the Internet, we would like to suggest that New Zealand works with key stakeholders, partners and allies – both nationally and internationally – towards this purpose.
- We would also like to support your objective towards “multi-stakeholder participation in the negotiations.” For InternetNZ, it is important that Internet governance conversations become ever-more inclusive and broadly based, so that the perspectives of those using the Internet can be part of the process of shaping its development. We appreciate that there might be instances where the government will need to make decisions, but we also believe that these decisions are better informed if the views of other stakeholders are taken on board.
- Finally, we would like to express our full support in your effort “to consider the interests of, and potential impact on Māori and indigenous peoples internationally”.

InternetNZ stands ready to support, assist and collaborate with the New Zealand government throughout these negotiations. Internally, we will also be following these conversations and do whatever we can from our end to ensure that the process is inclusive and transparent.

If you would like to discuss these issues further with us, please contact me in the first instance to organise this ^{s9(2)(a)} [REDACTED]

In closing, I thank you again for this public consultation and for the opportunity to submit our comments.

Ngā mihi nui,

^{s9(2)(a)} [REDACTED]


Jordan Carter

Chief Executive

[REDACTED]

Introduction

1 What is your name?

Name:

s9(2)(a)

2 What is your email address?

Email:

s9(2)(a)

3 Are you answering on behalf of yourself or an organisation? - If organisation, please specify

Organisation:

Myself

Principles and objectives

4 Do you have any overall views about New Zealand's engagement in negotiations on the cybercrime convention?

Views on NZ's engagement:

New Zealand must take part in the negotiations to protect a free and interoperable internet. At the same time, negotiations must allow for a path of rehabilitation for perpetrators of cybercrime, and not be strictly punitive.

5 What do you think about the draft principles for New Zealand's engagement in negotiations?

What do you think - principles:

The draft principles for NZ's engagement in negotiations consider and provide for a range of good things.

6 Do you have any amendments or additions you'd like to make to the suggested principles for New Zealand's engagement?

Amendments/additions - principles:

The only criticism I would have would be in regards to the principle about helping the participation of the Pacific Islands. I would prefer for "seek to" to change to "endeavour to encourage and support", raising the threshold to better include our Pacific neighbours.

7 What do you think about the draft New Zealand objectives for negotiations?

What do you think - objectives:

I agree with the list of New Zealand's broader values for cyberspace. States need to better mobilise an international response to cybercrime, and the objectives work towards that. I especially like the consideration of indigenous people.

8 Do you have any amendments or additions you'd like to suggest for the draft objectives?

Amendments/additions - objectives:

In regards to indigenous interests and impacts, perhaps a more focused objective should be implemented - specifically regarding Māori and other indigenous groups' mātauranga and intellectual property.

9 Are there any particular issues you think are missing from this document?

Anything missing:

10 Is there anything else you would like us to consider?

Anything else:

Next steps

11 Are there particular areas you would like to highlight as key priorities or areas of interest for you in this process?

Areas of interest:

That the eventual convention supports and upholds New Zealand's broader values for cyberspace, as listed in the Draft Principles and Objectives document.

12 Would you like to discuss any of your feedback or the process more broadly directly by email, phone, VTC, or in person (COVID alert levels permitting)?

No

13 Would you be interested in being consulted again as negotiations unfold? (checking "no" here does not exclude you from future engagement, should you wish to reengage)

Yes

Official Information Act 1982

14 If you think there is a reason why anything in your submission should not be made public, please let us know here.

OIA:

15 If you are an individual, as opposed to an organisation, we will consider removing your personal details from the submission in the event of a request under the OIA. Are you happy for your personal information to be released?

Yes

Released under the Official Information Act 1982



21 October 2021

Tony Lynch
Deputy Chief Executive (National Security Group)
Department of the Prime Minister and Cabinet

Tēnā Koe Tony,

**RE: KĀPUIA FEEDBACK ON NEW ZEALAND'S DRAFT PRINCIPLES AND OBJECTIVES FOR
NEGOTIATING A NEW UNITED NATIONS CONVENTION ON CYBERCRIME**

Kāpuia appreciated the opportunity to provide feedback on **New Zealand's Principles and Objectives for Negotiating a new United Nations (UN) Convention on Cybercrime**. The Secretariat canvassed member feedback through an online survey, and I am pleased to share with you the collated feedback as a contribution to the work officials are undertaking to prepare the negotiations mandate on the new convention for Cabinet.

The members that responded support New Zealand's draft principles for engagement in the process, but would like to share the following considerations that could make the document stronger:

- New Zealand should also look to work with partners who have dissimilar interests, or "swing states", to bring them closer to what New Zealand and like-minded partners are thinking;
- for those less familiar, clarification could be added to explain how countries are considered to be like-minded;
- New Zealand should seek advice from academics, technology experts and business leaders;
- an amendment could be made to include wording that would encourage:
 - a transparent and inclusive process;
 - clarity that "multi-stakeholder" includes communities voices; and
 - the seeking of views that reflect New Zealand's multicultural landscape, as well as those of communities vulnerable to cybercrime.

Likewise, New Zealand's draft objectives for the new UN convention were generally considered to be fit for purpose, but they could be improved by:

- including the impact on Māori and indigenous peoples internationally, and the impact on vulnerable (including youth and elderly) and minority groups;
- improving cooperation amongst governments to minimise the impact of policies on victims of cybercrime;
- improving information provided to customers globally on online risks when they purchase an ICT device;
- clarifying a range of harmful online activity that is currently not illegal, but harmful so that harm that currently sits in the grey-zone can be addressed and victims have better information on where they can go.

Kāpuia is interested in receiving updates on progress towards forming a new convention, and:

- how the convention is considering “fake news” within the larger ecosystem of mis- and disinformation;
- efforts to minimise the currency of mis – and disinformation online relating to vaccines,
- efforts to counter foreign interference in New Zealand, at both Government and community levels and support being provided to affected communities;
- efforts to facilitate conversations or promote educational resources for ethnic communities in New Zealand to grow their knowledge on cybercrime; and
- progress on programmes to support youth who are susceptible to being influenced online.

You also asked Kāpuia how community interests could be better protected in future. The Secretariat shares the following points raised by some members for officials working on cyber and reducing online harm to consider more generally:

- While there is recognition of the impact of cyber-crime on victims, the scope of work should be widened to ensure victims feel supported and for a level of trust to be built so those directly affected feel they can engage as active stakeholders in the process of improving the system.
- System improvements regarding harmful online behaviour should be occurring in parallel to the negotiations of the new international convention and that more consideration should be given to educating the wider public on both identifying and protecting themselves against cybercrime.
- Where elements of the system are working well to educate communities, such as ‘The Eggplant’ initiative to support young people understanding the internet, there should be further promotion of these initiatives and other initiatives that are simple and accessible to a diverse range of people.

Thank you again for the opportunity for Kāpuia to provide its advice on the proposed convention at this early stage.

Ngā mihi

s9(2)(a)

Rosalind Plimmer

Kāpuia - Head of Secretariat

Submitted to New Zealand's draft principles and objectives for negotiating a new UN convention on cybercrime
Submitted on 2021-10-05 15:48:08

Introduction

1 What is your name?

Name:

s9(2)(a)

2 What is your email address?

Email:

s9(2)(a)

3 Are you answering on behalf of yourself or an organisation? - If organisation, please specify

Organisation:

On behalf of myself and my colleagues s9(2)(a)

Principles and objectives

4 Do you have any overall views about New Zealand's engagement in negotiations on the cybercrime convention?

Views on NZ's engagement:

Submission for UN Convention on Cybercrime

s9(2)(a)

Centre for Defence and Security Studies

Massey University

Overview

The submission authors all teach and research in areas of cybersecurity as part of their academic roles at the Centre for Defence and Security Studies (CDSS) at Massey University. We recognise the global and domestic urgency of addressing cybersecurity and cybercrime. Broadly, we are supportive of international efforts towards reducing cybercrime and encourage New Zealand's participation in those efforts. However, we find that this consultation process is lacking in context, in part because of New Zealand's underdeveloped position on the issue. This impacts our ability to provide informed input. We have consequently focused our feedback and suggestions around the key issues that we see arising from this process. This document is divided into three sections giving feedback on the consultation document.

Section One: Understanding New Zealand's contribution to countering international cybercrime through a proposed UN Convention.

Section Two: Ensuring that our domestic cybersecurity policy and national security policy are aligned across government to support our international efforts.

Section Three: Ensuring that consultation processes are fit for purpose and that a public dialogue around cybersecurity as a national security issue is maintained.

Each section contains critical comments with corresponding suggestions for addressing those comments. Lastly, given the critical importance of cybersecurity as a national security issue, we would welcome constructive dialogue between CDSS and MFAT on any future aspect of this process.

Section One: Understanding New Zealand's contribution to countering international cybercrime through a proposed UN Convention. We need to be more fully informed about the extent of New Zealand's capability, capacity, and intentions to be able to contribute actively and proactively to international cybercrime matters. Specifically, we are interested in understanding:

1. To what extent is New Zealand's participation in the UN Convention aligned with our regional leadership and priorities?

We strongly support the principle for the strongest mandate to support the UN Convention because New Zealand and the region are extremely vulnerable to cybercrime. Given how commonplace cybercrime is in NZ and throughout the Pacific today, a UN convention could offer an alternative form of protection for our citizens and region. However, care needs to be taken in balancing our participation in rules-based UN innovations with protecting our regional interests and longstanding alliances. For example, there are potentially injurious implications for New Zealand's current cyber security agreements and commitments internationally if we are not involved in these sessions. But we need to balance our position somewhat with our own national views and with those of our close partners. How will participation benefit and protect our Pacific region partners, for example? Does our position align with Australia with whom our internet is closely connected? Should it align? In preparation for a stocktaking meeting in Vienna in April 2021, our Australian partners suggested that: "...a new UN convention on cybercrime [is] not required for States to make progress combatting cybercrime and its impacts on society ..." Likewise, there has been an Exchange of Letters between New Zealand and the Government of the Socialist Republic of Vietnam constituting an Agreement regarding Cyber Security under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership. How will this exchange be impacted?

More broadly, there are some fundamental differences in how the West (Europe and the US) view governance in cyberspace compared to countries such as China, Russia, and Iran. What is New Zealand's stance on these differences and how will it address them at the various meetings given the aspirational goal of consensus is unlikely to be achieved? It would be beneficial to have a clear vision of how New Zealand's participation in the convention is aligned with our existing regional responsibilities and how any inconsistencies between these will be managed.

2. New Zealand's position on the Budapest Convention and other agreements.

It is important to understand the current agreements to which New Zealand belongs and the implications of how our future participation in the UN Convention might interact with those agreements (e.g. Budapest Convention and the Christchurch Call). Currently, the document does not outline the other agreements to which New Zealand is party to when it comes to cybersecurity and cybercrime. There are major divergences in how states tackle cybercrime and how they secure data including international security alliances and agreements, domestic and regional internet governance, international online content access and proprietorship. According to the Global Initiative, "[t]he [UNGA] policy agenda on cyber issues is highly fractious, with tensions over keeping cybersecurity and cybercrime separate and keeping cybersecurity off the formal Security Council agenda." Moreover, "if this process does lead to a convention, it will have major implications globally. Much depends on how the boundaries of the treaty are drawn..." It is not clear where New Zealand sits in terms of regional agreements and these tensions.

UN Resolution 74/247 does not invalidate existing agreements such as the United Nations Convention against Transnational and Organised Crime and the Budapest Convention on Cybercrime. However, ongoing concerns have been aired since its inception in 2019 about how well this Convention will integrate concurrent International Expert Group (IEG) recommendations and conclusions in that it "may not necessarily reflect efforts to modernise existing international instruments, such as the draft Second Additional Protocol to the Budapest Convention." Additionally, objections to the 2019 draft resolution included concerns about the duplication of effort by other regional agreements, such as the Budapest Convention, and fears around the timeline of the UN initiative slowing counter-cybercrime efforts further and potentially being stymied by large powers when regional agreements might be timelier and more effective.

New Zealand was one of those objectors - originally voting against the 2019 UN Convention on Cybercrime. What were the reasons then, what has changed, how does this match with the Hon David Clark's recent support for the Budapest Convention, and why reconsider this UN convention now? Without answers to these questions, it is challenging to provide informed input into the consultation process.

We note that New Zealand's participation in the Budapest Convention is led by the Ministry of Justice. We understand that New Zealand has an invitation to join, but still has not signed up due to changes that need to be made to its Search and Surveillance Act 2012, the Mutual Assistance in Criminal Matters Act 1994, the Crimes Act 1961, and the Customs and Excise Act 2018." Based on the legislative changes that are in progress to join the Budapest Convention, will New Zealand have sufficient resource capability and capacity to adopt even more new and unknown regulations set out by a further convention? Given the work completed to date and the ongoing work required to participate in the Budapest convention, clarity is required that these work programmes are aligned and not duplicating efforts in different siloes of Government. There is no assurance in the consultation that these existing instruments have been taken into account and will be built upon in this process. It is important to understand the current agreements to which we belong and how participation in the UN convention interacts with those agreements, specifically the Budapest Convention.

3. What is New Zealand's position and plan for acting on the UN Convention?

We would like some clarity around New Zealand's goals for participation in the UN Convention. What is New Zealand's start point for the discussion? How do we manage participation in the Convention with our existing relationships - we know we are not going to achieve global consensus, how are we going to manage different perspectives on issues such as global governance of the internet? We note that the consultation documents state that we do not know what issues are going to be proposed for consideration. This is worrisome. What are we proposing or are we just waiting to see what everyone else proposes first? How do the proposed high-level principles and objectives translate to the development of a Convention? Clear guidance on our position would allow participants in the consultation process to provide more informed contributions to facilitate better policy decisions.

Section Two: Ensuring that our domestic cyber-security policy and national security policy are aligned across government to support our international efforts.

We are concerned that this process as it currently stands is not fully aligned with other domestic national security agencies. We outline four issues below that we think need resolving. They are:

1. This document defines a vision of cybersecurity that does not match the vision that is outlined in the 2019 DPMC cybersecurity strategy. The source for this new vision is not made clear. Given that there are several Government agencies (not to mention NGOs and the private sector) working in relation to Cyber security, another vision intended simply for this UN Convention seems counterproductive. A unified vision that is clearly aligned with both the 2019 cyber security strategy and across Government would be a worthy objective.

2. We note that this consultation process is led by MFAT, who are working with DPMC and the Ministry of Justice. We would expect that the two agencies primarily responsible for New Zealand's cybersecurity (the GCSB and MBIE) would be involved as well. We would also expect that in terms of crime, there would be consultation with Police and DIA in addition to the Ministry of Justice. Given that the proposed vision is aimed at ensuring our 'national security is protected' it would be beneficial to provide evidence of a coordinated and integrated cross government approach to cybercrime/security and national security.

3. We also see disjunction in terms of responsibility for cybersecurity mirrored within the Government, with the Prime Minister, Ministers Kris Faafoi (Cyberstrategy), David Clark (the Budapest Convention) and Andrew Little (Calling out China) all variously publicly speaking about cybersecurity issues. At other times it has been the Director General of the GCSB Mr Andrew Hampton who has called out actors such as Russia. It is not clear who is responsible for cybersecurity in terms of the executive. This will be further compounded with responsibility for this convention falling under the responsibility of

Minister Mahuta. A clear understanding of who is responsible for cybersecurity, and when, from the executive would improve clarity of vision and purpose.

4. We note that New Zealand has recently been very clear that its vision on cybersecurity is aligned with the Five Eyes. We see potential disjunction with the language in this proposal which positions New Zealand as a rules-based actor focused on human rights and international law with our partisan position in the FVEYS. It seems that our FVEYS intelligence sharing agreement has stretched to incorporate foreign affairs around cybersecurity and this may force us down a path that may conflict with our position on developing a Convention on cybercrime. How will this be resolved? The process needs to clearly relate our FVEY interests with our participation in the Convention. Failure to do this may undermine the legitimacy of our position and compromise our international standing and reputation.

Given that Andrew Little in 2018 stated that cybersecurity (and terrorism) are New Zealand's two primary national security risks, we argue that it is a worthy objective to consider developing clear cross-government collaboration in this space. Given that cybersecurity and cybercrime are simultaneously domestic and international issues it seems essential that domestic and foreign policy follow suit by being clearly aligned in this space. As such we make the following four suggestions for aligning domestic national security policy for cybersecurity:

1. That a unified vision is offered that is clearly aligned with the 2019 cybersecurity strategy and across the various Government agencies responsible for cybercrime.
2. That consultation is extended to include the GCSB, MBIE, DIA and NZ Police in their various capacities when it comes to cybersecurity and crime.
3. That the Executive considers and explains how it determines the Ministerial responsibility for Cybersecurity. The Minister for Broadcasting may not have the remit for addressing Crime or security issues in cyberspace. Perhaps it could be made part of the portfolio of the Minister Responsible for the GCSB, NZSIS, and Pike River Re-entry.
4. That clear guidelines are developed which demonstrate how New Zealand proposes to balance its commitments to global cybersecurity both as a member of the international rules-based order and as a partisan member of the FVEYS alliance.

Section Three: Ensuring consultation processes are fit for purpose and that a public dialogue around cybersecurity as a national security issue is maintained.

Within a democratic society, consultation is an important function that serves a variety of purposes from epistemic, democratic and ethical perspectives. Focusing on the epistemic perspective, consultation is seen as an important process of developing citizen and expert derived knowledge to support decision making at the policy level. We are concerned that the current consultation process on what is one of New Zealand's most significant national security risks, is a largely symbolic one that is being undertaken only for the sake of appearances or to meet due process requirements. In that sense, it may be unlikely to fulfil the broader purpose of developing knowledge to inform important decisions that will need to be taken in the development of a Convention. We outline three issues below that we consider need addressing:

1. Participants in the consultation process must be well informed and provided with the resources and respect to enable them to participate meaningfully. Unfortunately, the process in question is lacking in this respect from two perspectives. Firstly, the background information provided – a three-page document focused largely on process – is inadequate to allow those being consulted to fully understand the background to the issue at hand. Missing are a range of key documents (including but not limited to UNGA Resolutions 74/247 and 75/282) along with outcomes of key meetings (notably the UN Ad Hoc Committee organisational session of 10-12 May 2021 at which seven NZ representatives were present) which give all-important context and would ensure consultation participants start with a common understanding of the issue. Secondly, and in line with the background document, the two-page document advising high level and draft principle and objectives, some of which are abstract the point of meaningless (e.g., '...supports a harmonised, modern global framework for the criminalisation of specific cybercrime and cyber-enabled crime offences...' p. 2), is also inadequate to allow those being consulted to provide meaningful input into New Zealand's proposed way forward. Of particular concern is the statement that "we do not know what issues are going to be proposed for consideration" (p. 2) which seems like an extremely reactive approach – does NZ simply plan to turn up and see what happens? We note that the Russian Federation has already submitted a draft convention for discussion at the first session in January 2022 – does NZ plan to do something similar? In terms of process, we would expect NZ to be proactive in such important discussions and have a proposed way forward in place which could be enhanced through the consultation process.

2. Consultation is a complex process which should be ongoing and involve various methods of engagement, (multi-stakeholder workshops, roundtables, presentations, etc) not just formal documents and written responses. Approaching the consultation process as a system, made up of many different methods, all of which interact, affect each other, and contribute to the overall outcome can be a useful way of ensuring issues are understood and, thus, better outcomes are achieved. We consider that the current approach should include a range and mix of methods to achieve ethical, democratic, and epistemic outcomes which can enhance the quality of decisions that are likely to be made.

3. Consultation should be meaningful and democratically engaged not merely symbolic. We consider that the truncated process undertaken thus far is largely symbolic, occurring predominantly as part of due process requirements. Failure to undertake meaningful consultation can result in insufficient information needed to allow a thorough analysis of options; suspicion and lack of buy in to the consultation process; and, ultimately, less than optimal decisions and outcomes.

Noting the above comments, and given the significance of this issue, we make the following recommendations regarding ongoing and future consultation processes:

1. That participants are well informed on both background issues as well as on New Zealand's proposed way forward to allow them to provide informed input.
2. That consultation be ongoing and that a broader range and mix of methods are utilised to engage participants so as to ensure greater understanding and, thus, better outcomes.
3. That consultation be meaningful and engaged to ensure information can be provided which allows knowledge to be developed that leads to better policy decisions and outcomes.

Authors

s9(2)(a)

5 What do you think about the draft principles for New Zealand's engagement in negotiations?

What do you think - principles:

6 Do you have any amendments or additions you'd like to make to the suggested principles for New Zealand's engagement?

Amendments/additions - principles:

7 What do you think about the draft New Zealand objectives for negotiations?

What do you think - objectives:

8 Do you have any amendments or additions you'd like to suggest for the draft objectives?

Amendments/additions - objectives:

9 Are there any particular issues you think are missing from this document?

Anything missing:

10 Is there anything else you would like us to consider?

Anything else:

When we prepared our submission we were unaware that we would not be able to upload it as a file to the portal. As such, we have pasted our entire document into box 4. We can send a copy of the word document on request. We also note that the portal does not allow for multiple authorship and that our submission is multi-authored. The authors all teach and/or research in Cybersecurity and are as follows:

s9(2)(a)

Next steps

11 Are there particular areas you would like to highlight as key priorities or areas of interest for you in this process?

Areas of interest:

12 Would you like to discuss any of your feedback on the process more broadly directly by email, phone, VTC, or in person (COVID alert levels permitting)?

Yes (we will contact you on the email address provided to arrange a further discussion)

13 Would you be interested in being consulted again as negotiations unfold? (checking "no" here does not exclude you from future engagement, should you wish to reengage)

Yes

Official Information Act 1982

14 If you think there is a reason why anything in your submission should not be made public, please let us know here.

OIA:

15 If you are an individual, as opposed to an organisation, we will consider removing your personal details from the submission in the event of a request under the OIA. Are you happy for your personal information to be released?

Yes

Submission on New Zealand's Draft Principles and Objectives for Negotiating a New UN Convention on Cybercrime

Introduction

This submission is made by Mega Limited, New Zealand registered company, no. 4136598, ("MEGA"). No part of this submission is private or confidential.

MEGA is an end-to-end encrypted cloud storage and chat service provider with over 235 million registered users in 250 countries and territories who have uploaded more than 106 billion files, with internet traffic exceeding 800 Gbps.

Although MEGA's head office is based in Auckland, MEGA operates globally. Consequently, MEGA has extensive experience with overseas disclosure and Mutual Legal Assistance Treaty ("MLAT") requests as well as local requests in relation to cybercrime activities.

Mega is branded as 'The Privacy Company' as it provides enhanced privacy compared to other platforms because of its user-controlled end-to-end encryption. Mega seeks to support the Universal Declaration of Human Rights, Article 12:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence[...]. Everyone has the right to the protection of the law against such interference[...]."

However, Mega has zero tolerance for illegal activity and is widely commended by both local and international law enforcement agencies in regards to its compliance and disclosure processes, in relation to requests for assistance by relevant law enforcement agencies in regard to serious criminal cases.

By way of further background on MEGA and its experience in dealing with illegal material online, including that which may be related to cybercrime activities, copies of MEGA's most recent Transparency Report, its Terms of Service ("ToS") and its Takedown Guidance Policy ("TGP") are attached in the Appendix to this submission. MEGA would note in respect of such attached material that:

- It is a common feature of cloud storage services to allow the sharing of user



files, and MEGA is no different. Users can establish folder shares with other MEGA users or export URL links to files and folders. If anyone makes a link public, e.g. by posting it to a forum, members of the public, rights-holders and law enforcement agencies will be able to see the content that is linked to. If that content is illegal and is reported to MEGA, it is dealt with in accordance with MEGA's ToS and TGP. MEGA works with law enforcement agencies in New Zealand (including the Department of Internal Affairs and Police) and overseas (e.g. the FBI in the US and EuroPol in the European Union) both to have content removed and to provide information for tracing and evidence for prosecution.

- MEGA links are disabled and user accounts closed (access barred and all existing links disabled) depending on the nature of the content and infringement (copyright) or illegality.
- The percentage of infringing/illegal file/folder links notified to MEGA is extremely small, currently averaging around 0.0002% of all files uploaded.
- Like any cloud storage provider, users can encrypt, upload to MEGA and then share content of an illegal nature despite that being a fundamental breach of MEGA's ToS. MEGA continues to cooperate with law enforcement agencies in relation to the removal of such material and preservation of evidence for subsequent prosecution. However, as noted in MEGA's submission earlier this year on the Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill, there is uncertainty at present as to whether MEGA has legal authority to retain illegal material for evidentiary purposes once it becomes aware of it, even if requested to do so by law enforcement and other similar agencies.

MEGA's experience outlined above makes it uniquely placed to provide input on certain aspects of New Zealand's principles and objectives for negotiating a new UN Convention on Cybercrime ("UNCCC") as set out in the two page document entitled 'New Zealand's draft principles and objectives for negotiating a new UN convention on cybercrime' ("Principles and Objectives Document") which was provided to MEGA along with the invitation to MEGA to make a submission on the Principles and Objectives Document.

MEGA has responded in respect of the aspects of the Principles and Objectives Document that are particularly relevant to MEGA's experience and operations. The fact that MEGA has not responded on certain other aspects of the Principles and Objectives Document, does not imply any acceptance or rejection of, or any particular view on, those matters.



Improved Focus

It is stated on the first page of the three page document entitled 'The new United Nations convention on cybercrime' ("Background Document") provided to MEGA along with the invitation to MEGA to make a submission on the Principles and Objectives Document that:

"The convention will further enable international cooperation in the ongoing and increasingly complex fight against cybercrime. Beyond that, the shape and potential scope of the convention are unclear at this stage."

While acknowledging the above, as well as the statements on the second page of the Background Document that:

"At this stage, we do not know what issues are going to be proposed for consideration...We are therefore inviting interested parties to provide feedback on the proposed high-level principles and objectives which will guide our overall approach."

MEGA believes that the potential guidance afforded by the Principles and Objectives Document can still be improved, even at this early stage, in regards to the focus on certain matters that have the potential to go on and form key parts of the final UNCCC.

Draft principles for New Zealand's engagement in the negotiations

Technology Industry Consultation

In regard to the draft principles for New Zealand's engagement in the negotiations included in the bullet points on the first page of the Principles and Objectives Document ("Principles Bullet Points"), MEGA believes that consultation with, and the involvement of, the New Zealand technology industries should be a much more clearly defined principle.

MEGA notes that the third of the Principles Bullet Points states:

"Advocate for our interests, and work in close cooperation with a broad coalition of likeminded partners (on substance, approach to negotiations and outreach)."

Although this appears to signal a desire to consult widely in relation to conducting negotiations for the UNCCC, MEGA believes it does not do enough to acknowledge the



central role that the involvement of the New Zealand technology industries should play and in particular those companies which offer international online communication and storage services.

Service providers of all nature within the New Zealand technology industries will undoubtedly be the most affected by both the changes to existing laws and the creation of entirely new legal obligations within New Zealand domestic law, that are likely to be required for New Zealand to accede to a cybercrime focused convention, such as what the proposed UNCCC will eventually entail. It therefore makes sense to ensure that these parties likely to be the most affected are extensively consulted and involved in relation to the negotiation process.

There is clear precedent for the importance of such involvement by the New Zealand technology industry in matters of this nature. In regard to the Counter-Terrorism Legislation Bill currently before Parliament, which also has significant implications for particular sectors of the New Zealand technology industries, the risk of failing to consult with the technology industries was clearly highlighted at page 30 in the Regulatory Impact Statement 'Strengthening New Zealand's counter-terrorism legislation', completed by the Ministry of Justice in November 2020. Here it is stated:

"There is a potential for negative impacts on the Government's relationship with tech companies if there are additional costs to them and our lack of consultation with these companies in developing the proposal. This is a particular concern given Government is working closely with this sector as part of the work on the Christchurch Call."

By ensuring the New Zealand technology industries are given a key role in relation to advising on negotiations in respect of the proposed UNCCC, the government can also ensure it will be able to draw on the experience and insight of one of the most knowledgeable sectors with regards to the matters that will come up for discussion as part of the UNCCC negotiations. Drawing on this experience and insight would ensure that the government can not only be more accurate and efficient in what it advances as part of the negotiations, but can also be better resourced and prepared to counter any issues raised by other negotiating parties, which are adverse to New Zealand's interests in respect of the negotiations.

The eventual steps of working through required law changes and other domestic actions necessary for New Zealand to accede to the final UNCCC, will also likely be a more streamlined and less controversial process if the New Zealand technology industries are centrally involved in relation to the negotiations of the UNCCC from the outset. As the key sector likely to raise the most concerns and potentially make the most objections, if the New Zealand technology industries have already had the opportunity as part of the overall negotiation process to ensure that the most appropriate and relevant stance is being taken on the key issues involved, their suspicion of and objections to the final form



of the UNCCC and the actions necessary to bring that into New Zealand law, will likely be significantly reduced.

Industry and Statutory Bodies

As well as the involvement of the New Zealand technology industries being a much more clearly defined principle within the Principles and Objectives Document, MEGA additionally believes the importance of the involvement in relation to the negotiations for the UNCCC of pertinent industry and statutory bodies within New Zealand, should also be acknowledged. For example, InternetNZ and the Domain Name Commission are two industry bodies who will have knowledge and experience in regard to instances of and the effects of cybercrime in New Zealand. Any legislative changes which are subsequently sought to be put in place with respect to addressing cybercrime in relation to New Zealand acceding to the UNCCC, are likely to notably impact on these bodies and the constituents they work with and represent.

In terms of New Zealand statutory bodies, the Office of Film and Literature Classification plays a key role in New Zealand with regard to reviewing and classifying online material that can in some cases relate to various types of cybercrime. The Office of Film and Literature Classification would therefore also be well placed to provide quite unique insights on certain aspects of cybercrime which we face in New Zealand, which it should be ensured are taken into account as part of New Zealand's negotiations for the UNCCC.

With regard to New Zealand statutory bodies, MEGA also believes the Principles and Objectives Document should acknowledge the importance of the involvement of the Office of the Privacy Commissioner, in relation to the UNCCC negotiations. New Zealand has robust privacy legislation and an internationally respected reputation when it comes to dealing with privacy related issues. In no way is this better recognised, than by the fact that since December 2012, the European Commission has formally acknowledged that New Zealand's privacy law provides comparable privacy protection to European standards. This 'adequacy' status is something that only a very small number of other countries can also claim.

As well as being a glowing commendation for New Zealand's approach to privacy matters, on a more practical basis, New Zealand's adequacy status with the European Commission also means that personal information can be sent from Europe to New Zealand for processing, without the need for other measures to be taken. This is something all other countries who do not have this adequacy status must deal with. This is a significant competitive advantage for many New Zealand businesses and it should be a focus of New Zealand's negotiations, that the final form of the UNCCC does not contain anything, that if New Zealand were to accede to the UNCCC, could potentially compromise this very special status New Zealand has when it comes to the processing of European personal information. To assist in achieving this, the involvement of the Office of the Privacy Commissioner in relation to the UNCCC negotiations would be very important and should be clearly acknowledged in the Principles and Objectives Document.



Draft objectives for the new UN convention on cybercrime

Budapest Convention

In regard to New Zealand's draft objectives for the UNCCC included in the bullet points on the second page of the Principles and Objectives Document ("Objectives Bullet Points"), MEGA notes that the intention as stated in the second to last of the Objectives Bullet Points, is that the UNCCC:

"Does not conflict with or erode existing instruments, including the Budapest Convention on Cybercrime, but rather takes those existing instruments into account and builds on them."

MEGA believes that this objective in particular needs to take on a significant focus of New Zealand's negotiation efforts in regard to the UNCCC.

The Budapest Convention on Cybercrime ("**Budapest Convention**") which New Zealand is currently in the process of joining, entered into force on 1 July 2004 and has currently been ratified by 66 countries. With its objectives of ensuring the provision and harmonisation of domestic laws regarding cybercrime, as well as establishing an improved system for international co-operation in dealing with cybercrime, the Budapest Convention would appear to currently be essentially what the UNCCC is intending to become.

The Budapest Convention has been criticised by some countries such as Russia, India and South Africa and has also seen many countries join subject to reservations in respect of certain Articles. However, it is now well-established and since coming into effect has proven to be a reasonably effective mechanism in encouraging and providing for, international co-operation in meeting the challenges posed by cybercrime.

Consequently, from the outset of the negotiations for the UNCCC, a very clear objective for New Zealand should be ensuring the UNCCC does not look to unnecessarily replicate the successful elements of what the Budapest Convention has already established. MEGA strongly agrees that a key objective for the UNCCC, should be to work on building on the positive aspects of international co-operation in dealing with cybercrime that the Budapest Convention has already provided for, as well as looking to provide for positive action in any areas that the Budapest Convention may have proven to be deficient.

Mutual Legal Assistance Treaties

Notwithstanding the above comments regarding the respect that should be given to the Budapest Convention, when it comes to other existing instruments currently available to deal with instances of cybercrime, MEGA believes that the MLAT process currently in

place is unreasonably slow, and any changes to standardise, streamline and speed up the process would be beneficial for all parties concerned. To the extent that this is not done in relation to New Zealand's accession to the Budapest Convention, then this is an area MEGA believes the UNCCC should address. Consequently, MEGA believes that any objective New Zealand has for the UNCCC to:

"not conflict with or erode existing instruments"

should only involve respecting existing instruments to the extent such instruments are actually proving to be effective in the fight against cybercrime.

Access to Electronically Stored Evidence

In regard to the draft objective stated in the third to last of the Objectives Bullet Points that the UNCCC:

"Recognises that the relevance of digital evidence extends beyond cybercrime and cyber-enabled crime, and supports the improvement of access to electronically stored criminal evidence, to facilitate the resolution of a wide range of offences."

MEGA would question the need for such a specific objective for the UNCCC, given that such a concept is on the whole already adequately provided for under New Zealand and most other domestic laws by virtue of standard rules of evidence. MEGA would also note that any countries who have already acceded to the Budapest Convention, will have already had to provide within their domestic laws for mechanisms to ensure improved retention of and access to data and information relating to domestic and international criminal investigations. This would appear to be another case of where, rather than looking to create new standards and procedures in certain areas, one of New Zealand's key objectives for the UNCCC should be building on existing instruments such as the Budapest Convention, that are already providing for effective measures in these areas in the fight against cybercrime.

MEGA would also note that an objective that only focuses on:

"...the improvement of access to electronically stored criminal evidence..."

and fails to adequately acknowledge the need to also balance privacy considerations, as well as guard against the potential for any new processes to be utilised for inappropriate purposes, is far from appropriate as a goal for the final form of the UNCCC.

For example, unless it is a clear objective from the outset of the UNCCC negotiations to appropriately guard against such possible issues, there is the potential for any new processes under the UNCCC which provide for easier international access to electronic



data in criminal cases, to be abused by authorities in other UNCCC countries for inappropriate political purposes. Another UNCCC signatory country could, under the guise of pursuing computer related crime, seek to obtain data held by New Zealand companies relating to the actions or work of political dissidents from their country, in situations where the alleged criminality of the dissidents may be the result of legitimate challenges to legally questionable actions of the regime.

Even if the final form of the UNCCC does provide for safeguards against such possible actions, the fact should not be down-played that eventual accession to the UNCCC will likely legitimise and formalise processes for access to data held in New Zealand by a range of international parties and on a scale, that has never been available before. Importantly, given the procedural framework that the UNCCC will likely adopt in such cases, (if the processes currently provided for in the Budapest Convention are a reasonable reference point,) it is also likely that such processes will be difficult for holders of data in New Zealand to legitimately resist. Consequently, these types of considerations need to be taken into account right from the outset in any objectives New Zealand has regarding the final form of the UNCCC.

MEGA has itself had direct experience of the above mentioned types of potential issues regarding politically motivated actions being dressed up as legitimate legal requests and then the use of established legal avenues by the party in question, to achieve the sought-after questionable outcomes. In 2016 the Kazakhstan Government, which was then under a significant cloud relating to claimed corruption and human rights abuses, obtained a disclosure order in a US Court based on claimed misuse of computers, for access to user data of individuals who had published MEGA links on social media which disclosed improper political activity. The Kazakhstan Government then enforced that order in the New Zealand Courts against MEGA, despite MEGA's strong objections.

The limitations of the objective stated in the third to last of the Objectives Bullet Points noted above with regard to access to electronically stored evidence, also needs to be considered with regard to the nature of the technology involved. For example, there are issues regarding access to information and data where such is secured by way of user-controlled end-to-end encryption, such as MEGA provides to its users. In such cases, regardless of what the legal framework provides for, the information and data involved will from a technological perspective simply be impossible to access, unless the user-password is known or the user created a publicly shared URL. Therefore, any objective of the UNCCC focused on providing better access to electronically stored evidence, would need, right from the outset, to also acknowledge that the nature of the actual storage technology involved in any specific case, will create unique issues compared with traditional physical evidence.



Framework and Resources

In regard to the draft objective stated in the third of the Objectives Bullet Points that the UNCCC:

“Addresses and improves international responses to emergent forms of cybercrime and cyber-enabled crime, including cybercrime as a service that require urgent collective action, such as sharing of harmful content online or ransomware.”

MEGA believes a better intent for such an objective would be to focus on providing the frameworks within which such actions will be taken, rather than looking to solely advance the specific responses themselves. New and emerging forms of cybercrime and cyber-related crime will continually pose new and often unique challenges that will need to be addressed. However, in MEGA’s experience in co-operating extensively with domestic and international law enforcement agencies, the key issues involved in dealing with more established forms of cybercrime and cyber-enabled crime, such as hacking and the creation and dissemination of terrorist or child exploitative material, are not overly different from dealing with newer and emergent forms of cybercrime.

In MEGA’s opinion, the main impediment to more effectively dealing with all types of cybercrime be they existing or new and emergent forms, comes down to failing to have appropriately established frameworks within which to do such and just as importantly, failing to appropriately resource such frameworks. When requested to provide evidence to international law enforcement agencies in regard to the investigation of cybercrime, the amount of information and data MEGA is able to provide in some cases can overwhelm the law enforcement agencies, who either do not have the manpower to deal with the volume of information and data supplied, or do not have the specialist skills necessary to most efficiently process such. The answer to such issues is at a basic level ensuring the establishment of specialist independent task forces or groups within law enforcement and the justice systems of countries, that are allowed to operate in ways most appropriate for combating cybercrime and just as importantly ensuring that such task forces and groups are appropriately resourced to deal with the volume and technical nature of crimes they will be investigating.

One of New Zealand’s objectives for the UNCCC should therefore be that the UNCCC requires the establishment and appropriate resourcing within each country, of law enforcement agencies to tackle all forms of cybercrime and cyber-enabled crime, be they already existing forms or new and emerging ones. If each country that accedes to the UNCCC needs to ensure that such frameworks are established and appropriately resourced, then decisions regarding what types of specific cybercrime or cyber-enabled crime should be focused on and the manner in which action is to be taken in respect of them, will be much easier to deal with.



Safe Harbours

MEGA believes a key objective that New Zealand should have for the UNCCC is that not only does it provide appropriate mechanisms to combat cybercrime, but that it also provides appropriate protection for those who chose, or are required, to assist in relation to such.

More specifically, MEGA believes that a focus of the UNCCC should be ensuring the provision of appropriate legal safe harbours to those individuals, companies and organisations who assist in the gathering, retention or analysis of evidence for cybercrime related prosecutions or take action in relation to such material when requested to by law enforcement or when they are otherwise required to by law.

An example from New Zealand of the type of issue MEGA would like to see the UNCCC include provisions to address, relates to the Films, Videos, and Publications Classification Act 1993 (“Classification Act”) and which has already been referred to in the Introduction to this submission. In New Zealand an internet service provider is provided protection by Classification Act from liability for possession or distribution of illegal material on its network, until it obtains actual knowledge of such material’s existence. However, at that point the Internet service provider needs to delete such material in order avoid liability. There is no protection under existing New Zealand law for an internet service provider who continues to store the illegal material at the request of law enforcement.

It is these types of issues that MEGA believes should be a key objective for the UNCCC to address and harmonise internationally, so that individuals, companies and organisations who are called on or otherwise chose to take appropriate action in regards to cybercrime related material, have confidence that their actions will not place them at any legal risk.

Reporting and Transparency

MEGA believes another key objective not currently mentioned in the Objectives Bullet Points that New Zealand should have for the UNCCC, is that any new processes and mechanisms established by virtue of the UNCCC in regard to combating cybercrime, are also coupled with appropriate transparency and reporting provisions. It would however still be appropriate that there were reasonable limits on such requirements, where the disclosure of certain details could jeopardise the investigation or prosecution of specific instances of cybercrime.

MEGA believes that such transparency and reporting requirements are essential in order to provide a check and balance on the use of any new law enforcement powers established by virtue of a country acceding to the UNCCC.

There is already potential precedent in New Zealand for such types of measures. For example, the annual Parliamentary reporting that it is envisaged will be required, in respect of the exercise of certain new data preservation order related powers which we



will need to provide for in our domestic legislation, in order for New Zealand to accede to the Budapest Convention.

s9(2)(a)



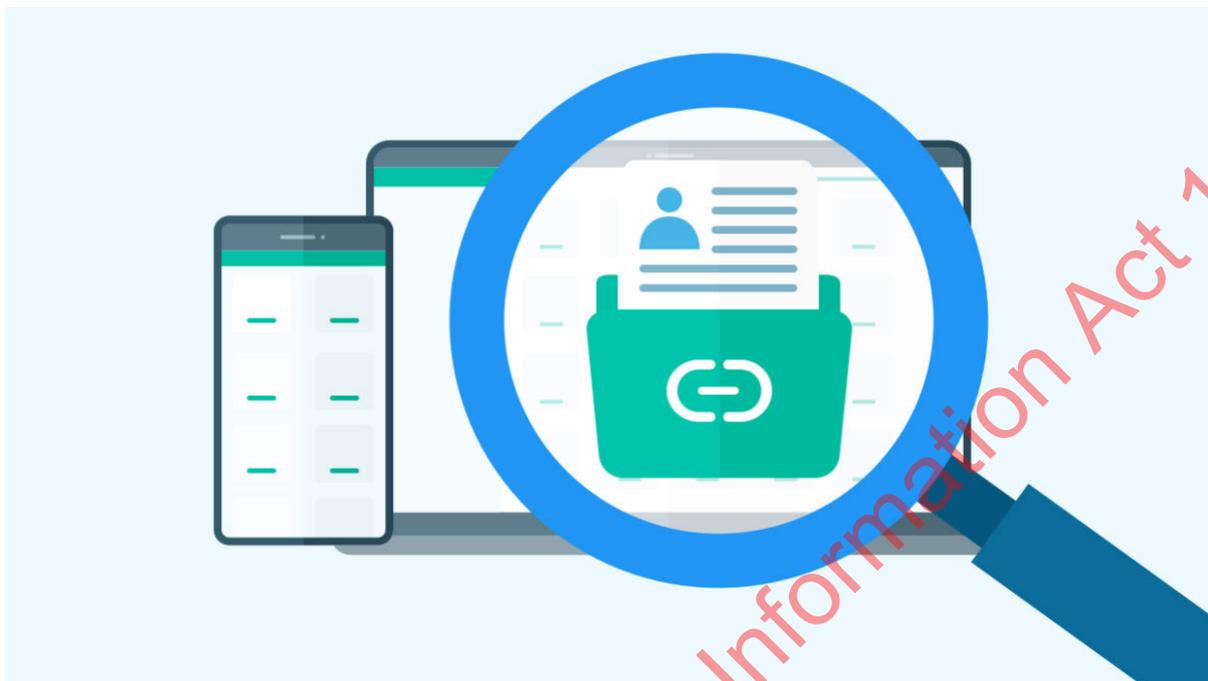
Stephen Hall
Executive Chairman – Mega Limited
6 October 2021

Released under the Official Information Act 1982



APPENDIX

Released under the Official Information Act 1982



Mega Transparency Report

September 2020

Requests for Removal of Content and for User Information

Report Issued 2 December 2020



Introduction

This is the sixth transparency report published by Mega since it commenced operations in January 2013. Today, Mega has over 200 million registered users in more than 200 countries and territories. In total, Mega's users have stored more than 87 billion files. In accordance with its [Privacy & Data Policy](#), Mega periodically publishes statistics on takedown requests, subscriber information disclosure and related issues.

In 2013, Mega pioneered user-controlled end-to-end encryption through the web browser. It provides the same zero-knowledge security for its cloud storage and chat applications, whether through a web browser, mobile app, desktop app or command line tool. MEGA The Privacy Company provides [Privacy by Design](#) with zero-knowledge user-controlled end-to-end encryption.

All chat messages and files stored on Mega are fully encrypted on the user's device, using keys encrypted with the user's password. The password remains on the user's device and is never sent to Mega, so chats and file contents can't be read or accessed in any manner by Mega. Files can only be decrypted by the original uploader through a logged-in account or by other parties who have consciously been provided with file/folder keys by the account holder.

Mega stores very limited non-encrypted Personal Data, such as the user's email address and some activity detail relating to account access, file uploads, shares, chats etc. A full description of the information Mega stores about a user and their activities on Mega's system can be found in clause 7.3 of Mega's [Privacy & Data Policy](#).

Regulatory Background

Mega was designed and is operated to ensure that it achieves the highest levels of compliance with regulatory requirements.

Mega's service is governed by New Zealand law and users submit exclusively to the resolution of any disputes by arbitration under New Zealand law. Mega has sought extensive legal advice on its service from lawyers in New Zealand and various other jurisdictions in order to minimise the risk of non-compliance with regulatory requirements in the primary locations in which it operates.

Mega maintains market-leading processes for dealing with users who upload and share copyright infringing material or breach any other legal requirements. Mega cannot view or determine the contents of files stored on its system as files are encrypted by users before they reach Mega.

However, if a user voluntarily shares a link (with its decryption key) to a folder or file that they have stored on Mega, then anyone with that link can decrypt and view the folder/file contents. Mega's [Terms of Service](#) provide that copyright holders who become aware of public links to their copyright material can contact Mega to have access to the offending files disabled.

By complying with the relevant provisions of New Zealand's Copyright Act, Mega is provided with a safe harbour, shielding it from liability for the material that its users upload and share using Mega's services. Although not technically bound by US or EU law, Mega also complies with the conditions for safe harbour under the US Digital Millennium Copyright Act ([DMCA](#)) process and the



European Union Directive 2000/31/EC. Mega does this by allowing any person to submit a notice that their copyright material is being incorrectly shared through the Mega platform. When Mega receives such notices, it promptly removes or disables access to the specified file or files, in accordance with Mega's [Terms of Service](#) agreed to by every registered user. The number of files which have been subject to such takedown notices continues to be very small, indicative of a user base which appreciates the speed and flexibility of Mega's system for legitimate business and personal use.

The safe harbours in various jurisdictions require material to be removed or links disabled expeditiously. Some cloud storage providers target takedown within 24 hours. Mega targets takedown within a maximum of 4 hours, with most takedowns being actioned within minutes.

When designing and implementing its takedown policy and processes, Mega consulted with New Zealand law enforcement authorities. Mega has adopted policies and processes which it has been advised are consistent with their requirements¹.

Mega has [Terms of Service](#) that have to be acknowledged by every new user before their account activation can be completed. Those Terms make it very clear (e.g. in clauses 13.6 and 17-20) that Mega won't tolerate infringement or any other illegal activity.

However, it is impossible for Mega to review content uploaded by users, as it is encrypted at the user's device before it is sent to Mega.

It is also logistically impossible for any cloud storage service (or indeed any other service provider in the Internet chain, such as the connectivity provider, browser supplier, etc.) to review all uploaded content due to the massive volume of data that transits these services. For example, Mega's users upload approximately 65 million files per day, 750 files per second on average. The infeasibility of policing user uploads has been clearly recognised in numerous court cases around the world.

Even if content could be reviewed, in many cases it would not be possible to determine whether it is infringing or not as the owners of many copyrighted materials provide the user with a licence to make a backup copy, so uploading it to a cloud storage service would not be infringing.

Other similar cloud storage services also don't attempt to assess the copyright status of uploaded materials

Requests for Removal of Content

Mega's approach to dealing with requests for the takedown of content uploaded by its users (as well as requests for the disclosure of user information and data) is set out in its [Takedown Guidance Policy](#).

¹ <https://mega.nz/terms>
<https://mega.nz/takedown>
<https://mega.nz/copyright>



Mega accepts takedown notices via a dedicated web page² or by email to copyright@mega.nz. Requests are promptly processed without reviewing their validity³.

The rights holder is able to specify one of three outcomes:

1. Removal of just a specified link to the file: - *the file will remain in the user's account;*
2. Removal of all links to the file: - *the file will remain in the user's account;*
3. Removal of all links to and all instances of the file: - *there is no user permitted to store this file under any circumstance worldwide.*

Folder links often refer to a large number of files, of which only some may be claimed to be infringing files. If the person requesting the takedown doesn't provide identification of the infringing file or files within the folder, Mega will disable the reported folder link as folder contents can change. This means that the folder and its files will remain active in the user's account. This would be the same as option (1) above in respect of file takedown requests.

Mega receives counter-notices from some users who dispute the validity of a takedown. These counter-notices are processed in accordance with safe harbour requirements. Most of the counter-notices Mega receives are genuine and appropriate. This is probably because many content owners and agents trawl the Internet using robots which generate incorrect notices on behalf of copyright owners, and due to the failure of owners and agents to review the specific link content.

The number of unique takedown requests submitted represents a very small percentage of the total number of files stored on Mega. In Q3 2020, the links taken down represented 0.0004% of the 84 billion files uploaded to Mega servers.

		Total Takedown Requests	Taken Down Links / Total Files	Total Files (Billion)
2018	Q4	67,315	0.0001%	52.8
2019	Q1	112,260	0.0002%	56.4
	Q2	118,780	0.0002%	60.0
	Q3	86,498	0.0001%	63.8
	Q4	145,640	0.0002%	68.0
2020	Q1	264,483	0.0004%	72.3
	Q2	471,055	0.0006%	77.6
	Q3	312,588	0.0004%	83.5

² <https://mega.nz/copyrightnotice>

³ It is impossible to review the validity as the file contents are user-encrypted (unless the user has published or provided the encryption key), and also due to the uncertainties of copyright status as noted above.



Takedown Processing



Figure 1 - Requests for file takedowns are a very small % of files uploaded

Repeat Infringers

Mega suspends the account of any user with 3 copyright takedown strikes within six months. In some cases, the account can be reinstated where it is proved to be the subject of invalid takedown notices, but most suspended accounts are terminated. As of 30th September 2020, Mega had suspended 94,966 users for repeated infringement. The data below shows that suspensions have declined to a very small % of the number of registered users.

Year	Quarter	Number of Suspended Users	% of Registered Users
2018	Q4	2,213	0.002%
2019	Q1	2,394	0.002%
	Q2	2,316	0.002%
	Q3	1,462	0.001%
	Q4	1,862	0.001%
2020	Q1	2,047	0.001%
	Q2	3,079	0.002%
	Q3	1,857	0.001%



Suspensions Resulting From Copyright Takedown Notices

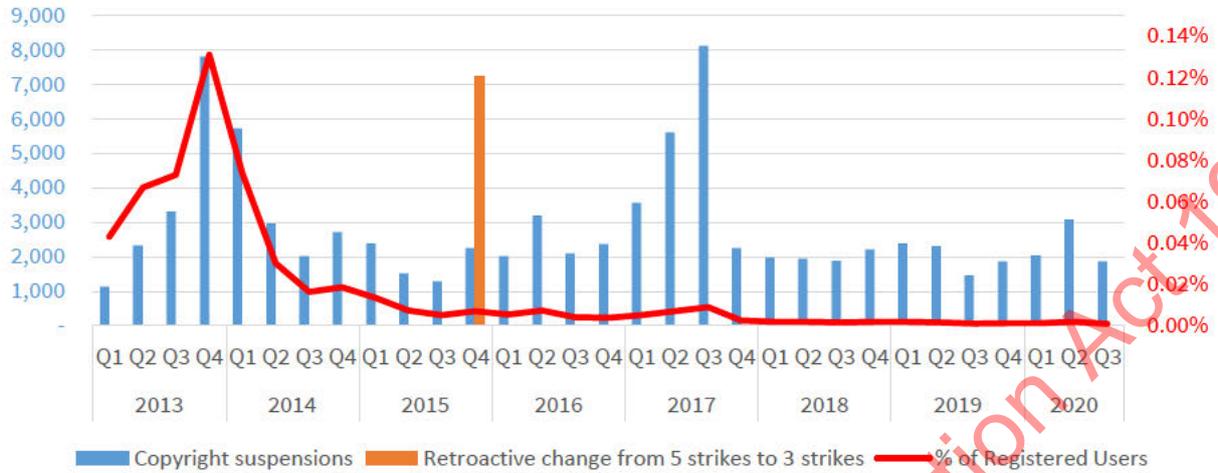


Figure 2 - Copyright Suspensions continue to be a very low % of registered users

Objectionable (Illegal) Content - Child Exploitation Material, Violent Extremism, Bestiality, Zoophilia, Gore, Malware, Hacked/Stolen Data, Passwords

Mega does not condone, authorise, support or facilitate the storage or sharing of Child Exploitation Material (CEM), also known as Child Sexual Abuse Material (CSAM) or other objectionable material as defined in section 3 of the New Zealand Films, Videos, and Publications Classification Act 1993 or other Internet-harming material. Mega has zero tolerance for users sharing such material. Any reports of such content result in immediate deactivation of the folder/file links, closure of the user's account and providing the details to the New Zealand Government Authorities for investigation and prosecution.

As of 30th September 2020, Mega had closed 565,000 accounts for sharing such content. The account information was made available to the relevant law enforcement agencies.

Appeals against account closure for holding alleged objectionable material are referred to the New Zealand Authorities for adjudication of the content. The account can be reinstated if the content is determined to be not illegal.

Mega is also a strong supporter of the 'Principles to Counter Online Child Sexual Exploitation and Abuse' issued in March 2020⁴. The Principles were produced by a working group of officials from New Zealand, Australia, the United Kingdom, the United States and Canada. Mega was one of the technology companies that provided supportive comment on the draft Principles during the consultation process.

⁴ <https://www.dia.govt.nz/Voluntary-Principles-to-Counter-Online-Child-Sexual-Exploitation-and-Abuse>



Court Orders / Warrants etc

During the year ended 30th September 2020, Mega was served 8 legal orders from NZ authorities and then disclosed account information for the relevant user accounts which are alleged to be involved in serious criminal activity overseas.

Other Requests for Personal Information

Mega is 'The Privacy Company' and values the privacy of its users. We are committed to maintaining industry-leading levels of security for, and confidentiality of, user data and information. In considering any request for access to such data or information, Mega starts from the position that user data and information is private and should always be protected to the greatest extent possible.

However, privacy and protection of user information and data are not absolute rights and are subject to some limitations, such as in cases of illegal activity.

The basis on which Mega may, in extremely limited situations, disclose user information and data is set out in Mega's [Takedown Guidance Policy](#).

Unless an Emergency Response (as defined below) is required, or disclosure is necessary in relation to an investigation involving CSAM or violent extremism, Mega will generally only provide user data or information when required to do so by New Zealand law, or by a New Zealand court or law enforcement authority with appropriate jurisdiction. Mega may consider requests made by non-New Zealand law enforcement authorities.

Mega defines Emergency Response as a situation where Mega has written assurance from a senior officer of the New Zealand Police or similar law enforcement officer or authority acceptable to Mega that in the expert judgment of such person there are valid reasons to believe that disclosure is necessary to prevent or lessen a serious threat (as defined in section 7(1) of the Privacy Act 2020) to:

- public health or public safety; or
- the life or health of an individual or individuals;

and the person giving such assurance confirms in writing that the threat is of such urgency that there is not time to obtain a production order or other court order.

If satisfied as to the above, Mega may, at its discretion, accept the request in good faith.

When Mega accepts a request, Mega will provide advance notice to the affected user unless prohibited by a court order or where Mega decides delayed notice is appropriate, based on criteria described in our [Privacy & Data Policy](#).



Although all files stored on Mega are encrypted prior to being uploaded to our system, and we therefore cannot access that content unless we are provided with the decryption key, Mega does have access to user registration information and the IP addresses used to access our services. A full description of the information Mega can retrieve about a user and their activities on our system can be found in clause 7.3 of our [Privacy & Data Policy](#).

The chart below shows the number of requests for subscriber information that have been processed since 2017.

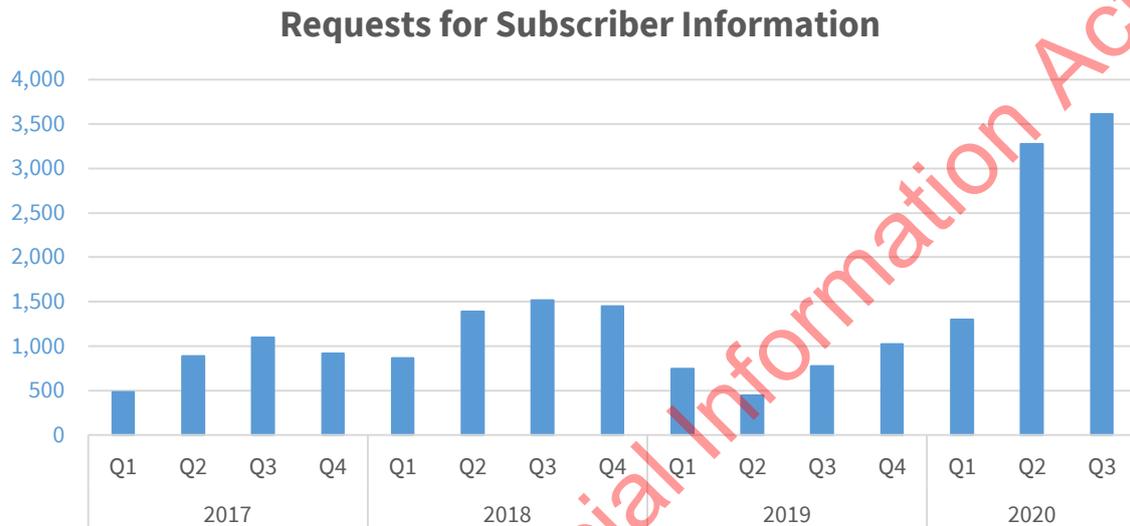


Figure 3 - Requests for Subscriber Information

During the 12 months from 1st October 2019 to 30th September 2020, there were also 7 requests for subscriber information that were declined by Mega, as they did not meet the necessary requirements set out in Mega's [Takedown Guidance Policy](#).

GDPR

The General Data Protection Regulation in Europe came into force in May 2018. Mega didn't need to make any substantial disclosure or make changes to its operations as privacy has been at the core of Mega's operations since it commenced in 2013.

In May 2018, we introduced a feature to allow users to download Personal Data relating to their account. There were quite a few requests in Q4 2018 but the number has reduced significantly since then.



GDPR Requests

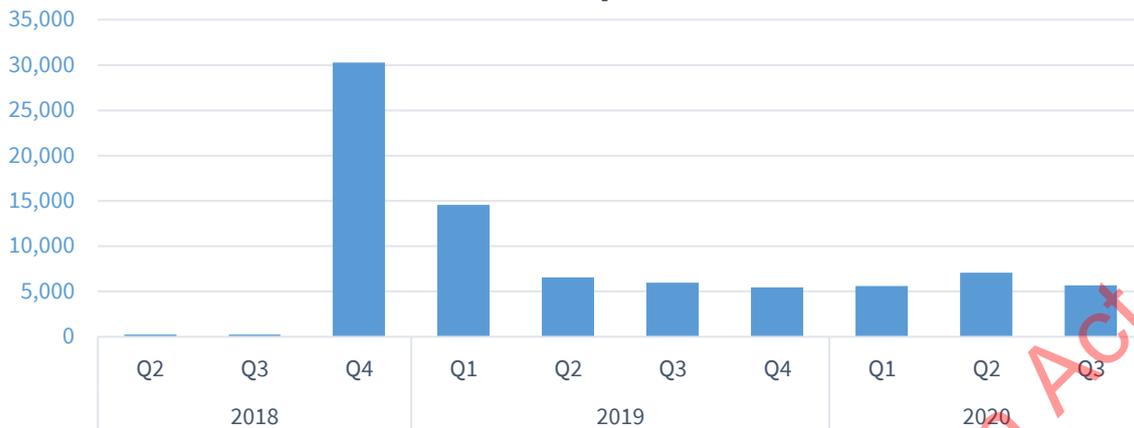


Figure 4 - User downloads of GDPR account information

Personal Data is retained indefinitely while the user's account is open. After account closure, Mega will retain all account information as long as there is any law enforcement request pending, but otherwise for 12 months after account closure, as users sometimes request that an account be re-activated.

After 12 months, identifying information such as email and IP addresses is anonymised (except that email address records are retained for reference by the user's contacts or where the user has participated in chats with other Mega users), but other related database records may be retained. This includes records of financial transactions relating to a user's account where Mega is legally required to retain such information.

When a user deletes a file, that file becomes inaccessible, is marked for deletion and is then deleted fully from the Mega system when the next appropriate file deletion purging process is run.

After account closure, all stored files will be marked for deletion and deleted fully when the next appropriate file deletion purging process is run.

Mega Limited, as controller, is represented in Europe by

Mega Europe sarl
4 Rue Graham Bell
L-3235 Bettembourg
Luxembourg
gdpr@mega.nz

The Lead Data Protection Supervisory Authority is the Luxembourg National Commission for Data Protection. This is the appropriate authority for accepting GDPR complaints about MEGA.

NATIONAL COMMISSION FOR DATA PROTECTION

15, Boulevard du Jazz
L-4370 Belvaux
Luxembourg
<https://cnpd.public.lu>



MEGA LIMITED TERMS OF SERVICE ("TERMS")

Scope of these terms	1-5
Your data	6-10
Your obligations	11-14
What you can't do	15-16
Our IP	17-18
Your IP	19
Copyright Infringement Notices	20-22
Copyright Counter-Notices	23-30
Other Infringement Notices	31
Suspension and Termination	32-36
Export Control	37
Severability and Waiver	38
Force Majeure	39
Disclaimers	40-47
LIMITATION OF LIABILITY AND INDEMNITY BY YOU	48-51
Disputes and Choice of Law	52-53
Business Accounts	54-57
Refunds	58
Recurring Paid Subscriptions	59
Cancellation of Recurring Paid Subscriptions	60
Information and Privacy	61-62
Notices	63
Rights to Third Parties	64
Entire Agreement	65

Scope of these terms

- 1 Welcome to Mega. Mega Limited ("Mega", "we", "us") provides cloud storage and communication services with user-controlled encryption. Using Mega, you and other users can encrypt your files and chats using user-controlled encryption ("UCE"), upload, access, store, manage, share, communicate,

download and decrypt files, chats and any data (all of which we call “**data**” in these terms) and give access to that data to others (all together, “**services**” and each, a “**service**”). We provide our services ourselves and via our **related or affiliated entities, payment processors and resellers** who act on our behalf, at our websites at <https://mega.nz> and <https://mega.io>, subdomains and related sites (“**websites**”), using our mobile apps (“**mobile apps**”), our desktop apps (“**desktop apps**”), our command line tools (“**cmd tools**”), our browser extensions (“**browser extensions**”) and our application programming interface (“**API**”). If you have questions about how to use our services or the great things you can do with Mega, check our **Help Centre** or, if you can't find the answer there, check our **contacts** page for details of who to contact.

- ② **Important:** We store all data on servers in New Zealand, Canada and Europe. If you access your data or give someone else access to your data using our services and you or they are not in New Zealand, Canada or Europe, you or they may be accessing that data from a country that does not give adequate protection to personal information when compared to that given under, the New Zealand Privacy Act 2020, the Canadian Personal Information Protection and Electronic Documents Act 2000 or the General Data Protection Regulation (“**GDPR**”). By agreeing to these terms, you authorise us to grant that access.
- ③ These terms are binding and apply to any use of the **services** by you and anyone who you allow to access your data or our services. By using our services, you and they irrevocably agree to these terms. If you do not like these terms or don't want to be bound by them, you can't use our services. In particular, OUR SERVICES ARE PROVIDED SUBJECT TO CERTAIN DISCLAIMERS BY US AND UNDERTAKINGS BY YOU, INCLUDING AN INDEMNITY FROM YOU IF YOU BREACH THESE TERMS - see clauses 40-51. NEW ZEALAND LAW AND ARBITRATION OF ANY DISPUTES APPLIES EXCLUSIVELY - see clauses 52 and 53.
- ④ We can change these terms at any time by providing you at least 30 days' prior notice of the change, whether via email or via a message in any service we provide. Your continued use after that notice means that you agree to the changed terms. If you have paid for a subscription that is due to expire after that 30 day notice period and you do not wish to continue to use our services under the new terms, you may terminate your subscription before the new terms come into force. We will then (but not otherwise) refund the unexpired portion of your subscription payment within 30 days and close your account. For more information about refunds, recurring paid subscriptions and their termination, see clauses 58-60.
- ⑤ If you comply with these terms, then we grant you a non-exclusive, non-transferable, worldwide licence to access and use our services, in accordance with these terms and any plan you have subscribed for.

Your data

- ⑥ If you allow others to access your data (e.g. by giving them a link to, and a key to decrypt, that data), in addition to them accepting these terms, you are responsible for their actions and omissions while they are using our services and you agree to fully indemnify us for any claim, loss, damage, fine, costs

(including our legal fees) and other liability if they breach any of these terms. This is particularly the case where you are the administrator of a business account (see clauses 33-35 and 54-57 below).

- 7 UCE is fundamental to our services. This means that you, not us, have encrypted control of who has access to your data. You should keep your password and Recovery Key safe and confidential. You must not share your password with anyone else and should not release encryption keys to anyone else unless you wish them to have access to your data. **If you lose or misplace your password, you will lose access to your data.** Encryption won't help though if someone has full access to your system or device. We strongly urge you to use best practices for ensuring the safety and security of your system and devices (e.g. via unique passwords, security upgrades, firewall protection, anti-virus software, securing and encrypting your devices). Mega will never send you emails asking for your password so do not be fooled by any such email since it will not be from us.
- 8 You must maintain copies of all data stored by you on our services. We do not make any guarantees that there will be no loss of data or the services will be bug free. You should download all data prior to termination of services.
- 9 Our service may automatically (without us viewing the file content) delete a file you upload, store, access or share where it determines that the file is an exact duplicate of a file already on our service (a process usually referred to as deduplication). In that case, the original file will be accessed by you and any other user and that file will be retained as long as any user has a right to access it under these terms. Any right of deletion that you exercise will not apply to a deduplicated file that is associated with another user.
- 10 We will store your data subject to these terms and any plan you subscribe to. If you choose to stop using our services, you must download your data first because after account closure we may, if we wish, delete all your data.

If we suspend or terminate our services to you because you have breached these terms, or someone you have given access to has breached these terms, during the term of that suspension we may, if we wish, delete your data immediately or deny you access to your data but keep it for evidential purposes. See also clauses 33-35 and 54-57 below which set out details of what happens to users within a business account when the business account is suspended or terminated.

In circumstances where we cease providing our services for other reasons, we will, if we consider it appropriate, it is reasonably practicable and we are not prevented by law or likely to incur any liability in doing so, give you 30 days' notice to retrieve your data.

Your obligations

- 11 Once you have subscribed to a plan for our services (with payment having been made via one of our websites, one of our mobile apps or one of our **related or affiliated entities, payment processors and resellers**), you need to continue to pay the fees (if any) for that plan (and any other taxes or duties). No matter which reseller or related or affiliated entity of Mega you make payment to, your contract for services is with Mega Limited and is governed exclusively by these terms and our policies referenced in these terms.
- 12 We can at any time change the fees for our services (other than those you have already paid for) and/or the terms of any services we provide to you (including without limitation the terms of any 'achievements', 'referral' or similar programs we may offer), as long as we give you (subject at all times to clause 34), 30 days' notice of any such changes. Where we change the fees for our services, in the absence of manifest error or other lawful error, you can't withhold payment or claim any set-off without getting our written agreement
- 13 If at any time you do not make a payment to us when you are supposed to (including on termination), we can (and this doesn't affect any other rights we may have against you):
- 13.1 suspend or terminate your use of the service and/or;
 - 13.2 require you to pay, on demand, default interest on any amount you owe us at 10% per annum calculated on a daily basis, from the date when payment was due until the date when payment is actually made by you. You will also need to pay all expenses and costs (including our full legal costs) in connection with us trying to recover any unpaid amount from you.
- 14 You must:
- 14.1 where you have subscribed for a service, always give us and keep up to date, your correct contact and any billing details and those of any users within a business account;
 - 14.2 comply fully with any account verification protocols we require you to follow, including account verification via SMS;
 - 14.3 comply with these terms and any other agreements you have with us and ensure that users within a business account, of which you are administrator, do likewise;
 - 14.4 comply with all applicable laws, regulations and rules when using our services and with respect to any data you upload, access or share using our services and ensure that users within a business account, of which you are administrator, do likewise.

What you can't do

- 15 You can't, and will ensure that no users within a business account, of which you are administrator:
- 15.1 assign or transfer any rights you have under these terms to any other person (including by sharing your password with someone else) without our prior written consent;
 - 15.2 do anything that would damage, disrupt or place an unreasonable burden on our service or anyone else's use of our service, including but not limited to denial of service attacks or similar;
 - 15.3 infringe anyone else's intellectual property (including but not limited to copyright) or other rights in any data;
 - 15.4 resell or otherwise supply our services to anyone else without our prior written consent;
 - 15.5 open multiple free accounts;
 - 15.6 make use of any additional services which are not meant to be available to you on the plan you have subscribed for (including without limitation additional storage or additional functionality) and for the avoidance of doubt, this includes where, for whatever reason, we may have provided you access to such services;
 - 15.7 use our service:
 - 15.7.1 to store, use, download, upload, share, access, transmit, or otherwise make available, data in violation of any law in any country (including to breach copyright or other intellectual property rights held by us or anyone else);
 - 15.7.2 to send unwelcome communications of any kind (including but not limited to unlawful unsolicited commercial communications) to anyone (e.g. spam or chain letters);
 - 15.7.3 to abuse, defame, threaten, stalk or harass anyone, or to harm them as defined in the [Harmful Digital Communications Act 2015 \(NZ\)](#) or any similar law in any jurisdiction;
 - 15.7.4 to store, use, download, upload, share, access, transmit, or otherwise make available, unsuitable, offensive, obscene or discriminatory information of any kind;
 - 15.7.5 to run any network scanning software, spiders, spyware, robots, open relay software or similar software;

- 15.7.6 to upload anything or otherwise introduce any spyware, viruses, worms, trojan horses, time bombs or bots or any other damaging items which could interfere with our, or anyone else's, network, device or computer system;
- 15.7.7 to use any software or device which may hinder the services (like mail bombs, war dialing, automated multiple pinging etc.);
- 15.7.8 to attempt to gain unauthorised access to any services other than those to which you have been given express permission to access; or
- 15.7.9 to impersonate anyone or to try to trick or defraud anyone for any reason (e.g. by claiming to be someone you are not).
- 16 If you register with us, you will need to use a password in conjunction with your specific account email address. You need to make sure your password is secure, not used by you on other sites and confidential. Make sure you tell us straight away if you think or know someone else has used your password or there has been any other security breach. We will hold you responsible for anything done using your account and password. MAKE YOUR PASSWORD A STRONG ONE AND KEEP IT SECURE. We are not responsible if someone else gains access to your computer or other device and/or your Mega password and/or encryption keys for any files.

Intellectual Property

Our IP

- 17 You are not allowed to, and you can't let anyone else (including in particular any user within a business account of which you are administrator), use, copy, alter, distribute, display, licence, modify or reproduce, reverse assemble, reverse compile, communicate, share, transmit or otherwise make available (whether digitally, electronically, by linking, or in hard copy or by any means whatsoever), any of our code, content, copyright materials, intellectual property or other rights without getting our permission in writing, other than in order to use our services as intended or as allowed under any open source licences under which we use intellectual property provided by others. The open source code that we use, where we obtained it, and licences for that code, are all referenced on our websites and via our mobile apps.
- 18 Without limiting any other provision of these terms, you are only permitted to directly and specifically use the API if you register at the developer registration page and agree that you may only publish or make available your application after we have approved it pursuant to our application approval process and licence agreement available on request at api@mega.nz

Your IP

- 19 You own, or undertake that you are authorised to use, any intellectual property in any data you store on, use, download, upload, share, access, transmit or otherwise make available to or from, our systems or using our services. You grant us a worldwide, royalty-free licence to use, store, back-up, copy, transmit, distribute, communicate, modify and otherwise make available, your data, solely for the purposes of enabling you and those you give access to, to use our services and for any other purpose related to provision of the services to you and them.

Copyright Infringement Notices

- 20 We respect the copyright of others and require that users of our services comply with copyright laws. You are strictly prohibited from using our services to infringe copyright. You may not upload, download, store, share, access, display, stream, distribute, e-mail, link to, communicate, transmit, or otherwise make available any files, data, or content that infringes any copyright or other proprietary rights of any person or entity.
- 21 We will respond to notices of alleged copyright infringement that comply with applicable law and are properly provided to us. If you believe that your content has been copied or used in a way that constitutes copyright infringement, please provide us with the following information:
 - 21.1 a physical or electronic signature of the copyright owner or a person authorised to act on their behalf;
 - 21.2 identification of the copyrighted work claimed to have been infringed;
 - 21.3 identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit us to locate the material including the exact URL link (with decryption key) to that material on Mega;
 - 21.4 your contact information, including your address, telephone number, and an email address; a statement by you that you have a good faith belief that use of the material in the manner complained of is not authorised by the copyright owner, its agent, or the law; and
 - 21.5 a statement that the information in the notification is accurate, and, under penalty of perjury (unless applicable law says otherwise), that you are authorised to act on behalf of the copyright owner.

- 22 We reserve the right to remove data alleged to be infringing without prior notice, at our sole discretion, and without liability to you. In appropriate circumstances, we will also terminate your account if we consider you to be a repeat infringer. Details of our designated copyright agent for notice of alleged copyright infringement are on our [contacts](#) page.

Copyright Counter-Notices

- 23 We process all takedown notices based on good faith acceptance of the representations from the party submitting the takedown notice. We do not review the material before processing the takedown notice.
- 24 You may file a counter-notice if you believe that access to a file you have uploaded has been wrongly disabled because it was the subject of an incorrect takedown notice. You should only do so if you are confident that no other party owns copyright in the material, or you have rights to store the material and, if you are sharing it, that you have the right to do so.
- 25 Please understand that:
- 25.1 when we receive your counter-notice, we pass it, including your address and other contact information, to the party who issued the original takedown notice. By submitting your counter-notice you authorise us to do so;
 - 25.2 filing a counter-notification may lead to legal proceedings between you and the complaining party;
 - 25.3 there may be adverse legal consequences in New Zealand and/or your jurisdiction if you make a false or bad faith allegation by using this process;
 - 25.4 if, when using this counter-notice process, you make a false or bad faith allegation or otherwise breach these terms or any of our policies and that causes us any loss, costs (including legal costs), damages or other liability, we reserve the right to claim for and recover from you that loss, those costs (including full legal costs on a solicitor-client basis), damages and other liability, by deduction from any balance in your account and/or by proceedings in New Zealand and/or the jurisdiction of the address in your counter-notice; and
 - 25.5 we provide this counter-notice process voluntarily for the purposes of all applicable copyright takedown and counter-notice regimes in New Zealand and other jurisdictions, but, in doing so, we do not submit to any jurisdiction, law, tribunal or court other than those of New Zealand, as set out in these terms. We may amend, suspend or withdraw this counter-notice process at any time, provided that any counter-notices in train at that time shall continue to be processed.

- 26 By filing a counter-notice, you are deemed to have accepted the above terms. If you do not accept the above terms, do not file a counter-notice.
- 27 To file a counter-notice with us, you must provide a written communication at <https://mega.nz/dispute> or by email to copyright@mega.nz that includes substantially the following:
- 27.1 Identification of the specific URL(s) of material that has been removed or to which access has been disabled;
 - 27.2 Your full name, address, telephone number, email address and the username of your Mega account;
 - 27.3 The statement: "I have a good faith belief that the material was removed or disabled as a result of a mistake or misidentification of the material to be removed or disabled.";
 - 27.4 The reasons for that good faith belief, sufficient to explain the mistake or misidentification to the person who filed the original takedown notice;
 - 27.5 The statement "I will accept service of proceedings in New Zealand or in the jurisdiction where my address in this counter-notice is located, from the person who provided Mega Limited with the original copyright takedown notice or an agent of such person.";
 - 27.6 A scanned physical signature or usual signoff in an email or using our webform will be accepted; and
 - 27.7 Any comments you wish to provide.
- 28 We will only accept a counter-notification directly from the user from whose account a folder or file has been disabled. Counter-notifications must be submitted from the email address associated with that Mega account.
- 29 If we do not receive any further communication from or on behalf of the person who originally submitted the takedown notice, or any communication we do receive does not in our sole opinion adequately justify the original takedown notice, we may, but shall not be obliged to, reinstate the material in approximately 10-14 days provided we have no reason to believe that the material infringes copyright.
- 30 Nothing in this counter-notice section prejudices our right to remove or disable access to any material at any time, for any reason or no reason.

Other Infringement Notices

- 31 If you consider there has been some other infringement or breach of law, or of these terms, and wish to file a complaint, contact us at the relevant address on our [contacts](#) page. We will generally require the same amount of detail as set out above for copyright infringement notices. See also our [Takedown Guidance Policy](#).

Suspension and Termination

- 32 You can terminate your access to our services at any time by following the 'Cancel your account' link in the Account section of our websites or the Settings section of our mobile apps. However, we will not provide any part-refund for any allowance not used on any subscription you may have, other than under clauses 4 and 58. If you are a business account administrator you may also terminate access to any user within the business account.

- 33 We can immediately suspend or terminate your, and (as may be applicable) that of other users within a business account, access to our websites and our services without notice to you:

33.1 if you or they breach any of these terms or any other agreement you or they have with us;

33.2 at any time if you are not a registered user;

33.3 if you are using a free account and that account has been inactive for over 3 months; or

33.4 if we have been unable to contact you using the email address in your account details.

- 34 Without in any way limiting the other rights available to us pursuant to these terms to take such further action as we deem necessary in any case, we may temporarily suspend your account, where a pattern of access to your account suggests to us that the account may have been compromised. You will subsequently be required to provide such verification of your right to access your account, as we deem appropriate, before we will unsuspend your account.

- 35 We may also terminate, suspend or limit our services or any part of our services, for all users or for groups of users, without notice, at any time, and as applicable for any duration of time(s) that we specify, for any reason or no reason, provided that in any such cases, to the greatest extent permitted at law, we will have no liability to you in any regard as a result of any such actions.

- 36 All charges outstanding on your account must be paid at termination.

Export Control

- 37 You may not use, export, re-export, import, or transfer any software or code supplied as part of your use of our services: (a) into any United States or New Zealand embargoed countries; or (b) to anyone listed as a specifically prohibited recipient by the United States Government or the New Zealand Government. By using our websites and our services, you represent and warrant that you are not located in any such country or on any such list. You also will not use our websites or our services for any purpose prohibited by United States, New Zealand or any other law, including, without limitation, the development, design, manufacture or production of missiles, nuclear, chemical or biological weapons.

Severability and Waiver

- 38 If any provision of these terms is held to be invalid or unenforceable, the remaining provisions will remain in full force and effect. If we do not enforce any right or provision of these terms or if we in any instance grant any concession or indulgence, that will not be deemed a waiver of such right or provision or obligate us to grant any concession or indulgence to anyone else or to you again.

Force Majeure

- 39 We will not be liable by reason of any failure or delay in the performance of our obligations because of events beyond our reasonable control, which may include, without limitation, denial-of-service attacks, strikes, shortages, riots, insurrection, epidemics, pandemics, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labour conditions, earthquakes, material shortages, extraordinary internet congestion or extraordinary connectivity issues or failure of a third party host, (each a "**Force Majeure Event**"). Upon the occurrence of a Force Majeure Event, we will be excused from any further performance of the obligations which are affected by that Force Majeure Event for so long as the event continues.

DISCLAIMERS

- 40 WE DON'T GIVE YOU ANY WARRANTY OR UNDERTAKING ABOUT THE SERVICES WHICH ARE PROVIDED "AS IS". TO AVOID DOUBT, ALL IMPLIED CONDITIONS OR WARRANTIES ARE EXCLUDED AS MUCH AS IS PERMITTED BY LAW, INCLUDING (WITHOUT LIMITATION) WARRANTIES OF MERCHANTABILITY, FITNESS FOR PURPOSE, SAFETY, RELIABILITY, DURABILITY, TITLE AND NON-INFRINGEMENT.

- 41 We will try to give you access to our services all the time, but we do not make any promises or provide you with a warranty that the services will be without any faults, bugs or interruptions.

- 42 Whilst we intend that the services should be available 24 hours a day, seven days a week, it is possible that on occasions our services may be unavailable to permit maintenance or other development activity to take place or be periodically interrupted for reasons outside our control.

- 43 Information provided on our services will change regularly. We will try to keep the information up to date and correct, but again, we do not make any promises or guarantees about the accuracy of such information.
- 44 We do not warrant that the services will meet your requirements or that they will be suitable for any particular purpose.
- 45 You are the controller in respect of some data Mega holds about you and Mega is the processor, for GDPR purposes. Mega is the controller in respect of some other data. See our [Privacy and Data Policy](#) for more details. These terms, our [Privacy and Data Policy](#), our [Cookie Policy](#) and our [Takedown Guidance Policy](#) are the contract between us that governs our processing of that data. It is your sole responsibility to determine that the services meet the needs of you, your business or otherwise and are suitable for the purposes for which they are used.
- 46 We also aren't legally responsible for:
- 46.1 any corruption or loss of data or other content which you or anyone else may experience after using our services or any problems you may have when you access our services;
 - 46.2 devices or equipment that we do not own or have not given you;
 - 46.3 any loss or damage if you do not follow our reasonable instructions, these terms, our [Privacy and Data Policy](#), our [Cookie Policy](#) and our [Takedown Guidance Policy](#); and
 - 46.4 any actions or non-actions of other people which disrupt access to our services, including the
 - 46.4.1 content and nature of any data that you upload, access or share;
 - 46.4.2 content of ads appearing on our services (including links to advertisers' own websites) as the advertisers are responsible for the ads and we don't endorse the advertisers' products; and
 - 46.4.3 content of other people's websites even if a link to their websites is included on our websites or our mobile apps.
- 47 You warrant that if you are accessing and using the services for the purposes of a business then, to the maximum extent permitted by law, any statutory consumer guarantees or legislation intended to protect non-business consumers in any jurisdiction (such as the [Consumer Guarantees Act 1993](#) in New Zealand) do not apply to the supply of the services or these terms.

LIMITATION OF LIABILITY AND INDEMNITY BY YOU

- 48 TO THE MAXIMUM EXTENT PERMITTED BY LAW, WE (THIS INCLUDES OUR EMPLOYEES, OFFICERS, AGENTS AND AUTHORISED RESELLERS) ARE NOT LIABLE WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), EQUITY OR ON ANY OTHER GROUNDS TO YOU OR ANYONE ELSE FOR ANY DIRECT, INDIRECT OR CONSEQUENTIAL DAMAGE, LOSS, COST OR EXPENSE, DAMAGE TO PROPERTY, INJURY TO PERSONS, LOSS OF PROFITS, LOSS OF DATA OR REVENUE, LOSS OF USE, LOST BUSINESS OR MISSED OPPORTUNITIES, WASTED EXPENDITURE OR SAVINGS WHICH YOU MIGHT HAVE HAD, OCCURRING DIRECTLY OR INDIRECTLY FROM THE USE OR ABILITY OR INABILITY TO USE, OR RELIANCE ON, OUR SERVICES, AND BASED ON ANY TYPE OF LIABILITY INCLUDING BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), STATUTORY OR PRODUCT LIABILITY, OR OTHERWISE.
- 49 YOU SHALL INDEMNIFY US AGAINST ALL CLAIMS, COSTS (INCLUDING ALL OUR LEGAL COSTS), EXPENSES, DEMANDS OR LIABILITY, DAMAGES AND LOSSES WHETHER DIRECT, INDIRECT, CONSEQUENTIAL, OR OTHERWISE, AND WHETHER ARISING IN CONTRACT, TORT (INCLUDING IN EACH CASE NEGLIGENCE), OR EQUITY OR OTHERWISE, ARISING DIRECTLY OR INDIRECTLY FROM BREACH BY YOU OR ANYONE YOU GIVE ACCESS TO YOUR DATA, OF ANY OF THESE TERMS OR ANY POLICY REFERENCED IN THESE TERMS.
- 50 IF YOU ARE NOT SATISFIED WITH THE SERVICES, THEN YOUR SOLE AND EXCLUSIVE REMEDY IS TO TERMINATE YOUR USE OF OUR SERVICES AND THE CONTRACT YOU HAVE WITH US.
- 51 DESPITE THE ABOVE, IF ANY COURT OR OTHER COMPETENT AUTHORITY HOLDS US (THIS INCLUDES OUR OFFICERS, STAFF AND AGENTS) LIABLE FOR ANY MATTER RELATED TO THESE TERMS OR OUR SERVICES, OUR TOTAL COMBINED LIABILITY WILL BE LIMITED TO THE MOST RECENT SUBSCRIPTION AMOUNT YOU HAVE PAID TO US.

Disputes and Choice of Law

- 52 Any and all disputes arising out of this agreement, its termination, or our relationship with you shall be determined by binding arbitration under the Arbitration Act 1996 in Auckland, New Zealand, by one arbitrator who shall be a lawyer knowledgeable in relevant technology matters appointed by the President for the time being of the Arbitrators' and Mediators' Institute of New Zealand Incorporated (AMINZ) on a request by either you or us. The following terms apply to the arbitration in addition to those implied by New Zealand law:

52.1 Notice must be given to apply for any interim measure in the arbitration proceeding;

52.2 The arbitration proceeding will commence when a request is made to AMINZ to appoint an arbitrator;

- 52.3 The arbitration shall be in English. The Arbitrator shall permit the parties and witnesses to appear by videoconference that we will organise and pay for; and
- 52.4 We will pay the arbitrator's fees and expenses unless the arbitrator determines that you should meet some or all of those fees and expenses because your dispute is frivolous or vexatious.
- 53 The relationship we have with you under these terms and their interpretation and construction together with any dispute, suspension or termination arising out of or in connection with them, is governed exclusively by New Zealand law. Mega does not submit to any other jurisdiction other than New Zealand and New Zealand law. You and we submit to the exclusive jurisdiction of the New Zealand arbitral tribunals (and courts for the purposes of the enforcement of any arbitral award or appeal on question of law). The parties agree to enforcement of the arbitral award and orders and any judgement in New Zealand and in any other country.

Business Accounts

- 54 For business accounts, the administrator of that account can see and deal with the files and data associated with all users within that account (including any data and any personal information). In addition:
- 54.1 If the business account is suspended or terminated, the action will affect the data and personal information of every user within that account;
- 54.2 The administrator of the business account will be able to see and deal with, change or delete the files and data associated with every user within that account (including any of data and personal information); and
- 54.3 The administrator of the business account will be able to terminate any user's account within the business account, restrict or disable usage of the account, change any user's password and otherwise deny access to the account and all data and personal information and such users will then lose access to all their data and all personal information associated with their account.
- 55 In respect of payment for business accounts:
- 55.1 We will charge the credit card associated with the business account with the applicable fees (including for any specified minimum) at the monthly billing date, on a recurring basis;
- 55.2 Notwithstanding clause 55.1, acting at our sole discretion we will be entitled to offer such alternative payment methods and/or payment terms to you as we deem appropriate, provided

that where such alternative payment methods and/or payment terms have been accepted by you, we may subsequently revoke such alternative payment methods and/or payment terms on 30 days' notice to you; and

- 55.3 In the event that there is any dispute as to the amount of any payment due (for example in respect of the number of active users on your business account in any month) then our decision on such matter shall be final and binding, and in the absence of manifest error or other lawful error, you can't withhold payment or claim any set-off without getting our written agreement.
- 56 Where a business account recurring payment fails for any reason, after 7 days we may suspend the account and all users within that account until payment is made. If no payment is made within a reasonable period of time, we will be entitled to terminate the business account and all users within that account, in which case all data and personal information associated with those users and the account will be subject to deletion in accordance with these terms.
- 57 Business accounts are subject to a fair use policy as follows:
- 57.1 Business accounts are only to be used for business purposes;
- 57.2 Business accounts are intended for multiple users and are not to be held or used by one person;
- 57.3 Each user must comply with these terms. Any breach of these terms by one user will be treated as a breach of these terms in respect of the whole account;
- 57.4 Mega will not be liable to any business account user should the actions of another user within the account, including the administrator of the business account, cause any loss or damage to another user within the business account (including by way of deletion, amendment, sharing or any other dealing with data or personal information); and
- 57.5 Each user's use of the business service must be fair, reasonable and not excessive, as reasonably determined by us by reference to average and/or estimated typical per business user usage of the business service. We will consider usage to be excessive and unreasonable where it materially exceeds the average and/or estimated use patterns over any day, week or month (or other period of time as determined by us) ("**excessive usage**"). If we identify excessive usage or consider that usage patterns on any business account indicate that any of the usage is not for business purposes we may suspend, and after 30 days' notice, terminate any or all of the users or the whole business account, in which case data and personal information associated with those users and the account will be subject to deletion in accordance with these terms. Examples of such unreasonable usage patterns also include: making non-business data publicly available,

adding users who do not appear to Mega to be associated with the business, and uploading or sharing files from non-business related third party sites.

Refunds

- 58 Unless otherwise provided by New Zealand law or by a particular service offer, all purchases are final and non-refundable. If you believe that Mega has charged you in error, you must contact us within 90 days of such charge. No refunds will be given for any charges more than 90 days old. We reserve the right to issue refunds or credits at our sole discretion. If we issue a refund or credit, we are under no obligation to issue the same or similar refund in the future. This refund policy does not affect any statutory rights that may apply. If you have made a payment by mistake and have not used the subscription plan services, you must contact support@mega.nz within 24 hours. This will be acknowledged promptly and answered within 7 days.

Recurring Paid Subscriptions

- 59 Recurring subscriptions will renew indefinitely, either monthly or annually, based upon your chosen subscription period, unless the subscription is cancelled prior to a renewal date. For recurring subscriptions established via mobile apps using in-app-purchase platforms, you should refer to your app store account for details of the dates and terms of the subscription. Any other recurring subscription will renew on the same day of month as it was established, except in cases where the day is not available due to a short month, in which case the renewal date will be moved to the first day of the following month.

Cancellation of Recurring Paid Subscriptions

- 60 Recurring subscriptions established through the mobile app using in-app-purchase platforms should be cancelled through the relevant app store account directly. Any other recurring subscription should be cancelled by navigating to <https://mega.nz/account> in your browser while you are logged into your account and selecting the option to cancel your subscription. Any payments processed after an effective subscription cancellation will be promptly refunded by us. If you cancel a paid subscription, but you maintain your Mega account as a free account, access to your account may be restricted or blocked if the level of use is above the limits applying to free accounts at that time.

Information and Privacy

- 61 We reserve the right to disclose data and other information as required by law or any competent authority. Our approach is referenced in our [Privacy and Data Policy](#) and [Takedown Guidance Policy](#), both of which are subject to these terms.

- 62 You and anyone else you give access to are also bound by our [Privacy and Data Policy](#), our [Cookie Policy](#) and [Takedown Guidance Policy](#). By accepting these terms, you also accept our [Privacy and Data Policy](#), our [Cookie Policy](#) and [Takedown Guidance Policy](#).

Notices

- 63 You can contact us by sending an email to support@mega.nz. If we need to contact you or provide you with notice we will email you at the email address you have recorded in your account details and such notices will be valid and deemed to be received by you whether or not you are using that address. We may also send notices via any chat facility or internal messaging system we may provide.

Rights to Third Parties

- 64 Mega Limited employees, officers, agents, related companies and affiliates together with authorised suppliers of services to and authorised resellers of, our services, are entitled to the benefit of all indemnities and other provisions of these terms which are for the benefit of Mega in these terms.

Entire Agreement

- 65 These terms, our [Privacy and Data Policy](#), our [Cookie Policy](#) and [Takedown Guidance Policy](#), the terms of any plan you purchase and any other terms and policies expressly referenced in these terms, together constitute the entire agreement between us relating to your use of our services. From the date they come into force, in respect of any use of any of our services after that, they supersede and replace any prior agreement, arrangement or understanding between you and us regarding the use of our services. No agreement, arrangement or understanding alleged to be made between us, or representation alleged to be made, by us or on our behalf, to you, if inconsistent with these terms, shall be valid unless agreed to in writing by an executive officer of Mega Limited.

Last updated 18 December 2020, effective 18 January 2021.





Takedown Guidance Policy

Guidance on Requesting User Information or "Takedown" of User Data

Overview

MEGA is 'The Privacy Company' and values the privacy of the users of its services. MEGA is committed to maintaining industry-leading levels of security and confidentiality of user information and data. However, privacy is not an absolute right and is subject to limitations.

This guidance describes how MEGA will achieve that balance and the approach it will generally take to requests in criminal and civil actions against or involving its users. This guidance is aimed at providing transparency to everyone interested in MEGA's services and consistency in its actions.

THIS GUIDANCE DOES NOT CREATE ANY LEGALLY BINDING OBLIGATIONS ON MEGA AND MEGA BEARS NO LIABILITY WHATSOEVER FOR COMPLYING OR NOT COMPLYING WITH IT, AS IT SEES FIT, AT ANY TIME. ALL LIMITATIONS AND EXCLUSIONS OF LIABILITY SET OUT IN MEGA'S [TERMS OF SERVICE](#) APPLY EQUALLY TO THIS GUIDANCE. MEGA MAY AMEND, REPLACE OR WITHDRAW THIS GUIDANCE AS IT SEES FIT. WHERE THERE IS ANY INCONSISTENCY BETWEEN THIS GUIDANCE, MEGA'S [TERMS OF SERVICE](#), MEGA'S [COOKIE POLICY](#) AND MEGA'S [PRIVACY AND DATA POLICY](#), THE [TERMS OF SERVICE](#) WILL PREVAIL.

MEGA reserves the right, unless required otherwise by applicable law, to provide differing levels and categories of information in response to different requests.

Important: Persons making a request should first check with MEGA what information may be available, particularly before applying for a criminal law production order or using civil law procedures to obtain user information or data. For law enforcement, checking first is also important, since in some circumstances, such as particular urgency, MEGA may not require a court order for release of information and may be prepared (but shall not be obligated to) retain information while disabling user access to it, for evidential purposes.

MEGA may amend, replace or withdraw this guidance temporarily or permanently from time to time as it sees fit. MEGA will generally try to give advance notice if possible, before changes to this guidance come into effect.

This guidance will be publicly available, including by publication on MEGA's website. MEGA may also periodically publish a summary of requests received and actions taken under this guidance.

Guiding Principles

In considering any request for user data, user information or action involving a MEGA user, MEGA starts from the position that user data and account information is private, so disclosure is only warranted in cases of clearly illegal activity. MEGA notes that all stored files and all chats are user-encrypted so they are unreadable to any other party unless the user has created and shared a folder/file link, shared a folder to a contact, shared the account password or included another party in a chat.

Applicable law for the purposes of this guidance is New Zealand law. However, MEGA may, at its sole discretion and without submitting itself to any other jurisdiction's law or courts or tribunals, consider requests made by non-New Zealand law enforcement authorities and civil claimants, on such basis and to such degree as MEGA sees fit.

Even if the decryption key is provided to staff or otherwise publicly available, MEGA generally will not view, or attempt to view, files against which action is requested but it reserves the right to do so where the file decryption key has been provided if it considers review is necessary or appropriate. MEGA is not obliged to take action unless required to do so by applicable law but any action will be undertaken objectively, based only on the information provided by third parties, this guidance, its [Terms of Service](#) its [Cookie Policy](#) and its [Privacy and Data Policy](#). Where there is any inconsistency between those MEGA documents, the [Terms of Service](#) prevail.

MEGA will promptly inform the user of any action taken where practicable, provided it considers it appropriate or is required to do so by applicable law, and provided it is not legally prevented from doing so by a court or other authority with appropriate jurisdiction. Action taken might not be disclosed in cases where an appropriate law enforcement agency requests non-disclosure because the case is under active investigation.

Emergency Response

This is defined as a situation where, in the expert judgement of a senior officer of the New Zealand Police or similar law enforcement officer or authority acceptable to MEGA, MEGA has written assurance that the person making the request has valid reasons to believe that disclosure or action is necessary to prevent or lessen a serious threat (as defined in section 7(1) of the Privacy Act 2020) to

- public health or public safety; or
- the life or health of an individual or individuals;

and where the person giving such assurance confirms in writing that the threat is of such urgency that there is not time to obtain a production order or other court order.

If satisfied as to the above, MEGA may, in its discretion, accept a request in such situations in good faith. In doing so, MEGA will be relying on the assurances given by the person making such request and will look to them and their organisation to cover any costs, damages, penalties, compensation or other liability should that assurance turn out to be incorrect or wrongly given for any reason.

The information to be provided or action to be taken by MEGA shall be as specified by, and agreed with, the appropriately designated officer.

MEGA will provide the New Zealand Police and other agencies approved by MEGA with the mobile phone number and email address of contact person(s) who will act on behalf of MEGA in an emergency response situation.

Objectionable Material - Child Exploitation Material, Violent Extremism, Bestiality, Zoophilia, Gore, Malware, Hacked/Stolen Data, Passwords

MEGA does not condone, authorise, support or facilitate the storage or sharing of Child Exploitation Material (CEM), also known as Child Sexual Abuse Material (CSAM) or other objectionable material as defined in section 3 of the Films, Videos, and Publications Classification Act 1993 or other seriously harmful material.

As **The Privacy Company**, MEGA does not condone spreading of viruses/malware or hacking and leaking of private data, passwords, or confidential information or other internet-harming material.

MEGA may (but shall not be obligated to) take down or disable access to such material, close the user's account and provide account details and other data to the appropriate authorities as it sees fit.

Allegations of Copyright Infringement ("notice and takedown")

MEGA will act on copyright infringement "takedown" notices in accordance with its [Terms of Service](#).

Users are advised in MEGA's [Terms of Service](#), and when using the service, that they must comply with all laws including copyright and other intellectual property laws. This includes, but is not limited to, a warning when generating a link for sharing files/folders.

MEGA will publish on its website the information to be provided and statements to be made by copyright owners or their duly authorised agents/representatives, to notify MEGA of an alleged copyright infringement.

All copyright infringement "takedown" notices should be made via the specific webform at <https://mega.nz/copyright> published on MEGA's website or by email to copyright@mega.nz with all the information specified in clause 21 of the [Terms of Service](#).

The notifier of alleged copyright infringement will be given the option of requesting either removal of link(s) to an allegedly infringing file or removal of all file(s) relating to a specific link/URL.

For file links, the submitter is able to choose one of three options:

1. Disable the reported link - the file will remain in the user's account;
2. Disable all links pointing to the same byte sequence - the file will remain in the user's account;

3. Disable all links and remove all files from all accounts referencing the same byte sequence - there is no user permitted to store this under any circumstance worldwide.

Folder links can refer to a large number of files, of which only some are claimed to be infringing. If the submitter doesn't provide identification of the individual copyrighted works and files within the folder that are claimed to have been infringed, MEGA disables the reported folder link consistent with option (1) above. Rights-holders can submit type (3) takedown requests for specific files within a folder by obtaining the handles for specific files within a folder (*select file(s) and use the right-click Get link(s) function*).

You can read more about our Copyright Notice process [here](#). For information on responding to a Copyright Notice you have received from MEGA, go [here](#).

Allegations of Other Intellectual Property Infringement ("notice and takedown")

MEGA will act in response to allegations of other forms of intellectual property infringement (e.g. trade mark infringement) in broadly similar fashion as for copyright infringement, reserving to itself the same discretions, rights and protections.

Notices of alleged intellectual property infringement, setting out full details similar to those required for copyright infringement "takedown" notices should be sent to ip@mega.nz

Civil Court Action for Alleged Copyright or Other Intellectual Property Infringement

Where a third party initiates court action against a MEGA user for alleged copyright or intellectual property infringement and wishes to access information held by MEGA for that purpose, the General Guidance above applies, i.e. this generally means a non party discovery order or, if that is not available, a witness summons, subpoena or agreed affidavit or statement of facts. Persons making civil requests should strictly comply with the New Zealand District Court or High Court Rules.

Other Cases

Other than as set out above in those specific situations, MEGA will generally only take action when required to do so by applicable New Zealand law or a court or law enforcement authority with appropriate jurisdiction, although it reserves the right to do so at any time and for any reason or no reason, as set out in its [Terms of Service](#)

For criminal matters, this generally means a New Zealand 'production order' as per Subpart 2 of Part 3 of the Search and Surveillance Act 2012 is required rather than simply a formal or informal request for information and/or action.

For civil matters, this generally means a New Zealand court non-party discovery order or, if that is not available, a witness summons, subpoena or agreed affidavit or statement of facts. Persons making civil requests should strictly comply with the New Zealand District Court or High Court Rules.

The information to be provided or action to be taken by MEGA shall be as specified in the relevant law or order, subject to MEGA being technically able to provide that information or take that action. As noted above, persons making criminal or civil information requests should contact MEGA first to see what information may be able to be provided.

Last updated 18 December 2020, effective 18 January 2021.

Released under the Official Information Act 1982

Submitted to New Zealand's draft principles and objectives for negotiating a new UN convention on cybercrime
Submitted on 2021-10-03 10:27:54

Introduction

1 What is your name?

Name:

s9(2)(a)

2 What is your email address?

Email:

s9(2)(a)

3 Are you answering on behalf of yourself or an organisation? - If organisation, please specify

Organisation:

Myself

Principles and objectives

4 Do you have any overall views about New Zealand's engagement in negotiations on the cybercrime convention?

Views on NZ's engagement:

I support the draft principles and objectives because they are well-grounded and recognise the key laws, principles and values of New Zealand that are pertinent to negotiating an international treaty on cybercrime.

I wish to make the following comments and suggestions as possible additions and further elaborations to the draft principles and objectives.

5 What do you think about the draft principles for New Zealand's engagement in negotiations?

What do you think - principles:

The draft principles are reasonable and sufficient.

6 Do you have any amendments or additions you'd like to make to the suggested principles for New Zealand's engagement?

Amendments/additions - principles:

- Principle to consider and provide for Māori interests can include Māori data sovereignty

This is an important principle. Matters and activities concerning cybercrime and digital investigations may have an impact on Māori data especially those held by government and companies. It is crucial then for Maori data sovereignty to be recognised in this principle. Māori data sovereignty refers to "the inherent rights and interests that Māori have in relation to the collection, ownership, and application of Māori data".

The principle can be amended to: "Consider and provide for Māori interests, the Crown's Treaty of Waitangi relationship, and the potential impact on Māori of issues including Māori data sovereignty INCLUDING MĀORI DATA SOVEREIGNTY arising in the negotiation process."

- Principle to advocate for a distinction between cybercrime and other cyber security matters may be expanded

This is a useful principle because it clarifies and delineates the scope of the new convention. It might be worthwhile to explicitly state that, together with cyber security matters, national security and intelligence issues are better discussed in a different forum. It would also be helpful to include the term "procedural law" since this, together with substantive criminal law, are the two main areas of cybercrime law.

The modified principle could state: "Advocate for a distinction between discussions on cybercrime (situated primarily in pure cybercrime, cyber-enabled crime, PROCEDURAL LAW and access to digital evidence) and other discussions on cyber security AND NATIONAL SECURITY AND INTELLIGENCE matters, which take place elsewhere in other UN processes (e.g. First Committee, not Third Committee)."

- Principle to advocate for a practical and future-proofed convention could incorporate the principle of technological neutrality

In order to ensure a practical and future-proofed convention, the principle of technological neutrality can be utilised. Technological neutrality requires "that legislation should define the objectives to be achieved and should neither impose, nor discriminate in favour of, the use of a particular type of technology to achieve those objectives".

This principle can be amended to: "Advocate for any eventual convention to be practical, TECHNOLOGY-NEUTRAL and future-proofed to the extent possible."

- A new principle can be added expressly recognising the values of law enforcement and human rights

A new Convention on Cybercrime will significantly impact and involve two important values: effective law enforcement and protection of human rights. These values are particularly relevant to cybercrime investigations and criminal procedure law (including search and surveillance).

It would be helpful to include a new draft principle about this, which could read: "RECOGNISE AND CONSIDER THE IMPACT ON THE VALUES OF EFFECTIVE LAW ENFORCEMENT AND PROTECTION OF HUMAN RIGHTS."

7 What do you think about the draft New Zealand objectives for negotiations?

What do you think - objectives:

The draft objectives are sound and achievable.

8 Do you have any amendments or additions you'd like to suggest for the draft objectives?

Amendments/additions - objectives:

- Objective that supports and upholds New Zealand's broader values for cyberspace could mention the right against unreasonable search and seizure and criminal procedure rights

In addition to the right to freedom of expression and right to privacy, the objective can also mention the right to unreasonable search and seizure and minimum standards of criminal procedure. The reason for the proposed inclusion is that the latter two civil rights are more germane to and directly impacted by cybercrime law, procedures and investigations. Further, freedom of expression and data privacy rights are subject to a general exemption for law enforcement. For example, the Privacy Act 2020 allows for non-compliance with a number of Information Privacy Principles "to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences". With regard to freedom of expression, the New Zealand Bill of Rights Act 1990 permits justified limitations including "reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".

The amended objective can read: "a well-functioning rules-based order in cyberspace that protects and promotes human rights including THE RIGHT AGAINST UNREASONABLE SEARCH AND SEIZURE, MINIMUM STANDARDS OF CRIMINAL PROCEDURE, the right to freedom of expression and the right not to be subjected to arbitrary and unlawful interference with privacy; and"

- Objective that supports a harmonised, modern global framework for the criminalisation of specific cybercrime may be expanded to refer to other categories of cybercrime

Under the Budapest Convention on Cybercrime, there are four general categories of substantive cybercrime: computer security crime, computer-related offences (such as computer-related forgery or fraud), content related offences (e.g., child pornography), and offences related to copyright and related rights. Cybercrime has also been classified as computer integrity crime, computer-assisted, and computer content crime. Using the same terms would assist in the harmonisation of international and national laws on cybercrime.

The objective could be modified to: "Supports a harmonised, modern global framework for the criminalisation of specific cybercrime, COMPUTER-RELATED, CONTENT-RELATED and cyber-enabled crime offences."

- Objective that recognises the relevance of digital evidence should also expressly uphold human rights

The purpose and intention of the objective is reasonable. However, any further or expanded access to and processing of stored criminal evidence should be subject to continued and potentially heightened human rights and legal protections.

The objective may be updated as follows: "Recognises that the relevance of digital evidence extends beyond cybercrime and cyber-enabled crime, and supports the improvement of access to electronically stored criminal evidence, to facilitate the resolution of a wide range of offences, BUT SUBJECT TO HUMAN RIGHTS AND LEGAL PROTECTIONS."

- Objective to not conflict with or erode existing instruments can also mention other relevant international treaties

Other international treaties that New Zealand has adopted or acceded to that are relevant to cybercrime and criminal procedure laws are the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, and bilateral mutual assistance treaties with other states. It would help to refer to these instruments as well.

The objective can be expanded to: "Does not conflict with or erode existing instruments, including the Budapest Convention on Cybercrime, THE UNIVERSAL DECLARATION OF HUMAN RIGHTS, THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS, AND MUTUAL ASSISTANCE TREATIES WITH OTHER STATES, but rather takes those existing instruments into account and builds on them."

9 Are there any particular issues you think are missing from this document?

Anything missing:

None.

10 Is there anything else you would like us to consider?

Anything else:

None.

Next steps

11 Are there particular areas you would like to highlight as key priorities or areas of interest for you in this process?

Areas of interest:

Substantive cybercrime and criminal procedural laws (including mutual assistance).

12 Would you like to discuss any of your feedback or the process more broadly directly by email, phone, VTC, or in person (COVID alert levels permitting)?

Yes (we will contact you on the email address provided to arrange a further discussion)

13 Would you be interested in being consulted again as negotiations unfold? (checking "no" here does not exclude you from future engagement, should you wish to reengage)

Yes

Official Information Act 1982

14 If you think there is a reason why anything in your submission should not be made public, please let us know here.

OIA:

None.

15 If you are an individual, as opposed to an organisation, we will consider removing your personal details from the submission in the event of a request under the OIA. Are you happy for your personal information to be released?

Yes

Released under the Official Information Act 1982

Department of Prime Minister and Cabinet

By email: Consultation@dpmc.govt.nz

6 October 2021

MICROSOFT'S SUBMISSION ON NEW ZEALAND'S DRAFT PRINCIPLES AND OBJECTIVES FOR NEGOTIATING A NEW UN CONVENTION ON CYBERCRIME

Background

- 1 The rapid increase in the availability of online services globally has led to significant growth in cybercrime. Promoting international cybersecurity measures is crucial to combatting cybercrime.
- 2 Given the nature of the online environment, Microsoft recognises that it is important that government, industry and civil society work together to prevent and address cyber-threats. Well-coordinated international and multi-stakeholder efforts are critical to ensuring at least a common baseline level of resilience and understanding across the globe.
- 3 New Zealand has experienced over the course of last year a number of cyberattacks, targeting organisations of fundamental importance to the country. Amongst others, publicly known victims of such attacks include NZ Stock Exchange (NZX), Reserve Bank of New Zealand, Waikato District Health Board, ANZ Bank, National Institute of Water and Atmospheric Research (NIWA) and others. These attacks, regardless of the motivations of the malicious actors, are becoming increasingly sophisticated and are growing in scale.
- 4 Microsoft is one of the leading cybersecurity organizations on the planet. Thanks to our scale, we receive threat intelligence from billions of data points, many times a day, from across all our cloud services – Azure, Office, Dynamics, Windows, Xbox, LinkedIn and others. This allows us to very comprehensively understand the global threat landscape and build security-by-design products and services. We are annually investing over a billion dollars in security alone and this spending will only increase – Microsoft CEO, Satya Nadella, committed at a meeting with US President Joe Biden in August 2021 that Microsoft will invest US\$20B in advancing security solutions over the next 5 years. This scale gives us a unique position to understand the nature of threats coming from both cybercriminal and state-sponsored actors.
- 5 The Council of Europe's Convention on Cybercrime ("Budapest Convention") is currently the only binding international instrument on cybercrime. It serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between parties to the treaty. In a public consultation in September 2020, Microsoft supported New Zealand joining the Budapest Convention. Cabinet has agreed that New Zealand will seek to join the Budapest Convention.
- 6 In December 2019, the UN General Assembly adopted resolution 74/247 establishing an "Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes". This resolution was followed in May 2021 with resolution 75/282 titled "Countering the use of information and communications technologies for criminal purposes" that set out the process for the

negotiations on the proposed cybercrime Convention. The process set out in Resolution 75/282 calls for a draft convention to be provided to the General Assembly at its 78th session (in 2023).

Support for the Budapest Convention

- 7 The Budapest Convention on Cybercrime entered into force in 2004. It harmonises Parties to the Convention's domestic laws on cybercrime to facilitate cooperation on criminal investigations. The provisions apply to cybercrime and criminal evidence that is stored electronically. The Budapest Convention also facilitates ongoing dialogue between Member States' to address cybercrime.
- 8 As per our submission to the Ministry of Justice and the Department of Prime Minister and Cabinet, Microsoft supports the Budapest Convention. We were encouraged by Cabinet's decision that New Zealand will join the Budapest Convention. Accession to the Budapest Convention will facilitate New Zealand's ability to effectively combat cybercrime and pursue mechanisms to access electronic evidence consistent with high standards of privacy and respect for digital sovereignty.
- 9 The new UN Convention on cybercrime should complement and build on, rather than replace, the Budapest Convention. In order to achieve greater impact, it is important that the proposed Convention does more than merely replicate existing efforts and instruments. However, it is equally important that the proposed Convention does not erode or undermine the Budapest Convention.

New Zealand's draft principles and objectives for negotiating a new UN Convention on cybercrime

- 10 Microsoft is broadly supportive of the draft principles and objectives. We have selected a number of the principles and objectives to comment on in more detail.

Principles

Consider and provide for Māori interests, the Crown's Treaty of Waitangi relationship, and the potential impact on Māori of issues arising in the negotiation process.

- 11 Microsoft supports reflecting in the negotiating position interests of all parts of the society and in particular Māori interests. We believe such an approach will provide New Zealand with a stronger mandate to advocate for the Convention to equally serve to protect indigenous peoples worldwide (as already considered in the draft objectives).

Advocate for a distinction between discussions on cybercrime (situated primarily in pure cybercrime, cyber-enabled crime and access to digital evidence) and other discussions on cyber security matters, which take place elsewhere in other UN processes (e.g. First Committee, not Third Committee).

- 12 Microsoft fully supports distinction between the discussions on cybercrime and responsible state behaviour in cyberspace. We believe these challenges, though related, should be discussed in separate UN structures and in line with their respective mandates.

Advocate for any eventual Convention to be practical and future-proofed to the extent possible

- 13 At a high level, Microsoft is very concerned about the overall, further fragmentation of global efforts to tackle cybercrime that this new instrument could bring. Throughout the negotiation, significant effort should be placed on preventing such an outcome.
- 14 We recommend that the overall scope of a potential new Convention be clearly and narrowly defined, and that it particularly focuses on "serious" crimes. Overall, it should not seek to expand the scope in an undue manner and it should complement rather than undermine existing provisions such as the Budapest Convention. Importantly, it should also not expand the scope to terrorism or other content-related offences. Nor should a new Convention endeavour to regulate industry – it should firmly focus on regulating the behaviour of States.
- 15 We recommend paying particular attention to discussions related to sovereignty and jurisdiction and ensure that any new draft facilitates the necessary co-operations rather than hinders or prevents them.
- 16 We recommend that the any new draft should seek to include adequate references to human rights, data protection laws, and also explicitly mention privacy rights.
- 17 Procedurally, we recommend that decisions related to this new Convention be taken by consensus and that, as mentioned elsewhere, negotiations allow for meaningful multi-stakeholder input.

Recognise the impact of cybercrime on victims and consider their interests in our approach to negotiations

- 18 Citizens need to be at the heart of discussions about the Convention. The focus of discussions should include ensuring the benefits of cyberspace are preserved for all users and that fundamental freedoms are protected. This also extends to political exception clauses, which should be included – that is, states should be allowed to refuse co-operation on the grounds of a political offence.
- 19 Overall, this Convention should be drafted in a manner that it protects *people from states*, rather than *states from people*.
- 20 The Convention and any domestic processes established under it must not impinge on the rights of individuals, law enforcement processes or technology generally.

Seek and encourage broad Member State and multi-stakeholder participation in the negotiations. This will not only ensure a more meaningful product, but will also ensure greater buy-in.

- 21 Microsoft fundamentally believes a multi-stakeholder approach is key in addressing challenges related to threats emanating from cyberspace, not least because cyberspace is owned and operated largely by the private sector. We take a note of a best practice developed

in New Zealand – the Christchurch Call and processes underpinning ongoing policy and operational work in this domain.

- 22 Microsoft believes that both industry and civil society have a crucial role to play in ensuring cybersecurity as well as combating cybercrime, and that all relevant negotiations will be improved by incorporating multi-stakeholder participation and perspectives. Moreover, effective cybersecurity capacity building programs rely on the support of government, industry, and civil society stakeholders with relevant expertise to develop trainings, exercises, and other initiatives.

Objectives

Addresses and improves international responses to emergent forms of cyber rime and cyber-enabled crime, including cybercrime as a service that require urgent collective action, such as sharing of harmful content online or ransomware.

- 23 While Microsoft appreciates the need to address emergent forms of cybercrime and cyber-enabled crime, we would strongly encourage caution in relation to including any “cybercrimes” that are focused on online content, given some of the particular human rights challenges that content-related crimes raise.
- 24 Great care will need to be taken through the negotiations process to ensure that human rights (including freedom of expression, privacy and access to information) are adequately protected through the Convention. Including any content related offences in the Convention as “cybercrime” raises a risk that the Convention becomes a shield for human rights abuses.
- 25 We recognize that the relevance of digital evidence extends beyond cybercrime and cyber-enabled crime, and supports the improvement of access to electronically stored criminal evidence, to facilitate the resolution of a wide range of offences. At a time when human interactions and activities take place online at an unparalleled scale, virtually every single crime in today’s world has a cyber element in it.
- 26 In line with Microsoft’s submission on the Budapest Convention, we recognise that obtaining digital evidence through traditional Mutual Legal Assistance Treaty processes can be slow and often ineffective for law enforcement. We believe the co-operation mechanisms available under the Budapest Convention go some way to resolving these issues.
- 27 Microsoft believes that modern bilateral and multilateral frameworks that allow for effective collaboration across the borders are best at addressing this challenge while preserving rights of the individuals. They also remove conflicts of laws which may occur in their absence. In this context, Microsoft encourages New Zealand to consider opening of negotiations for an Executive Agreement under the US CLOUD Act, once it completes its accession to the Budapest Convention.

Does not conflict with or erode existing instruments, including the Budapest Convention, but rather takes those existing instruments into account and builds on them.

- 28 As per our submissions above, it is important that the proposed Convention does more than merely replicate existing efforts and instruments. Conflicts between instruments should also be avoided.

- 29 In particular, Microsoft is concerned about the potential for any new Convention to undermine the Budapest Convention, which is internationally recognised as a best-practice response to cybercrime. Protecting other existing best practice international instruments (e.g., on counter-terrorism) should also be a priority in negotiations.
- 30 In Microsoft's view, there is an opportunity for greater collaboration between governments and private sector on the matters related to lawful data access. Most recently, the cloud computing industry from across various jurisdictions stressed how important such collaboration is in the industry's Trusted Cloud Principles. Microsoft believes that governments shall recognise the importance of resolving any existing conflicts of laws in alignment with the industry to maintain public trust in technology and the right to privacy.
- 31 Microsoft would like to also draw your attention to the recent *Multistakeholder Manifesto on Cybercrime: A call for responsible action and inclusion*, published by the Cybersecurity Tech Accord and Cyber Peace Institute. The Manifesto offers a unique, unified industry perspective on the matter.

Suggested additional principles and objectives

- 32 As outlined in our overall comments above, we encourage negotiators to have an additional core principle of seeking to ensure that human rights protections are clearly factored in at every step of the negotiations, and that rights to free expression, access to information and privacy are preserved. These important human rights should be enhanced, not eroded, by any new international instrument.

Kind regards,



Maciej Surowiec
Government Affairs Lead
Microsoft
s9(2)(a)



**THE NEW ZEALAND SOCIETY OF AUTHORS
TE PUNI KAITUHI O AOTEAROA (PEN NZ INC)**

October 2021

Submission to the Discussion on Cybercrime: Accession to the Budapest Convention

Background on NZSA:

1. The New Zealand Society of Authors Te Puni Kaituhi o Aotearoa (PEN NZ Inc) was established in 1934 and is the principal organisation representing and supporting Aotearoa New Zealand writers. We are a membership-based organisation representing 1,780 writers. NZSA is governed by a national board made up of an elected President and regional delegates including a Te Ao Māori board seat to represent and advocate for our Māori writers.
2. NZSA engages on a range of issues across government that affect writers and advocate for creative rights and fair reward,
3. NZSA is a member of International PEN and are active with Writers in Prisons NZ and international campaigns to protect the right to freedom of speech for imprisoned writers and journalists around the world. We produce a fortnightly e-news, monthly new books bulletins for our members and a quarterly NZ Author magazine and act as an information hub for the literary arts sector.
4. NZSA engages across the literary sector to ensure that the professional interests of writers are strongly represented and that early, mid-career and experienced writers receive support and career opportunities. Our representatives sit on a range of boards, committees, and steering groups such as PLR, CLNZ, Northtec, The Accessible Formats Coalition, PEN International, the Burns Fellowship Trust, the Book Awards Management Trust, Writers in Prisons, The Coalition for Books and We Create. We work with other organisations to further the work of NZ writers and the visibility of NZ books and literature.
5. NZSA is a 50% co-owner of Copyright Licensing NZ Ltd along with the Publishers Association of NZ and founding members of the Book Awards Trust and The Coalition for Books.
6. NZSA is a member of We Create, and we support submissions from that organisation.
7. Submitted by: Jenny Nagle, Chief Executive Officer, New Zealand Society of Authors Te Puni Kaituhi o Aotearoa (Pen NZ Inc), ^{s9(2)(a)} [REDACTED]

CYBERCRIME AND BUDAPEST CONVENTION

8. NZSA supports the New Zealand government principles and objectives in embarking on these international negotiations.
9. NZSA and PEN International are firm supporters of Freedom of Speech. We campaign for writers and journalists around the world who are persecuted for speaking truth. However, PEN and NZSA acknowledge that with Freedom comes Responsibility, and speech or actions that are harmful, should be subject to consequence.
10. While we know financial fraud and cybercrimes are rife and at front of mind for negotiators, we also wish our negotiators to consider digital copyright infringement. This is serious, widespread and affects NZ writers' incomes and wellbeing. It has never been so easy, in the history of the world, to digitise, copy and share work. Copyright infringement is also rife in cyberspace. We ask that negotiators remember the international copyright treaties NZ is signatory to, like the Berne Convention and Tripps.
11. NZSA believe that New Zealand Aotearoa's lack of legislation to curb internet giants is a fatal mistake. It appears that big tech as well as small ISP's are lawless and refuse to take steps to site block or infringe sites which infringe copyright. They universally ignore take-down notices. This lack of action and absence of accountability is harmful to creative rights and the creative sector.
12. We believe NZ safe harbours legislation for ISP's must be reviewed – and that the tech sector be made to take accountability for what is peddled on its sites – whether it be child porn, cybercrime, or creative works that infringe copyright, no entity should be unregulated and no entity should be above the law.
13. Our creative industries are formed on the bundle of rights granted under copyright law. The trading and licensing of those rights underpin the economics of the creative industries. NZ Aotearoa must be able to protect the IP of its creatives.
14. The government has marked the Creative Sector to be part of an Industry Transformation Plan. It sees great potential in our creative output and the growth of digital weightless product (gaming, film, TV, literature, music etc). We need a robust and secure digital infrastructure to support this growth.
15. NZSA and PEN International believe there is enormous political risk and potential social upheaval at stake from the rise of unchecked misinformation and fake news. This needs to be reined in, and managed, for the good of social cohesion.

Submitted to New Zealand's draft principles and objectives for negotiating a new UN convention on cybercrime
Submitted on 2021-10-01 16:19:45

Introduction

1 What is your name?

Name:

s9(2)(a)

2 What is your email address?

Email:

s9(2)(a)

3 Are you answering on behalf of yourself or an organisation? - If organisation, please specify

Organisation:

WeCreate Inc

Principles and objectives

4 Do you have any overall views about New Zealand's engagement in negotiations on the cybercrime convention?

Views on NZ's engagement:

We fully support New Zealand's engagement in the negotiations. The creative sector has, unfortunately, long and extensive experience with cybercrime. We recognise the absolute need for solutions to cybercrime and that those solutions will only be useful if they are the consensus views of all Member States.

5 What do you think about the draft principles for New Zealand's engagement in negotiations?

What do you think - principles:

We are pleased to see the inclusion of advocacy towards a convention that is practical and future-proofed. The history of digital technologies, including the development of the internet, has shown that predicting - and therefore future-proofing - regulatory and enforcement responses is complex.

The inclusion of a principle relating to the victims of cybercrime is also useful. The impacts and experiences for victims extend from personal/social, to cultural, moral and economic. All of these factors need to be taken into account.

When considering the resources made available to advocate for New Zealand's interests, consideration must also be given to what is at stake for New Zealand from cybercrime. As the country's economic mix (including exports) shifts from primarily physical goods to digital products and services, the potential damage to our people and our businesses from cybercrime increases. We suggest that the DPMC and MFAT may wish to undertake an assessment of the resourcing being put towards physical versus digital trade and ensure that this is adapted to sustain the level of support appropriate for each.

6 Do you have any amendments or additions you'd like to make to the suggested principles for New Zealand's engagement?

Amendments/additions - principles:

As above

7 What do you think about the draft New Zealand objectives for negotiations?

What do you think - objectives:

We support the objectives as drafted and note that the protection and promotion of human rights includes the rights for creative people to the protection of the moral and material interests in their creations.

A cyberspace that is safe, secure, stable, multi-stakeholder-governed, free, open and interoperable is an objective that seems a very long way from the cyberspace the world has today. There are thousands of publications available that document how we came to have the digital world that has evolved in the past quarter century, and that we can look to for examples of both the good, and the significant harms. Advocates for the "free and open internet" continue to ignore and underestimate the impact on many groups in society that an unregulated online world has enabled. The creative sector has breadth and depth of experience with this that we will be happy to share as engagement on the convention progresses.

8 Do you have any amendments or additions you'd like to suggest for the draft objectives?

Amendments/additions - objectives:

As above

9 Are there any particular issues you think are missing from this document?

Anything missing:

It would be helpful to understand how local stakeholder engagement will be facilitated during the development of the convention. It will be essential for the NZ negotiating team to have a reference panel to support their understanding of cybercrime, including emerging issues.

10 Is there anything else you would like us to consider?

Anything else:

Digital creation and online distribution of creative content and services are significant opportunities for New Zealand. They also create new and challenging risks through unauthorised uses, predominantly through hosting and distribution of illegal content on overseas websites or sharing via other technologies. There are few effective remedies available to content creators at either a local or international level in circumstances where their assets (their IP) have been stolen. As mentioned above, as NZ moves further towards an economy that derives much of its value from cyber-business, the safe and secure operation of cyberspace takes on even greater importance.

Next steps

11 Are there particular areas you would like to highlight as key priorities or areas of interest for you in this process?

Areas of interest:

Intellectual property enforcement mechanisms

12 Would you like to discuss any of your feedback or the process more broadly directly by email, phone, VTC, or in person (COVID alert levels permitting)?

No

13 Would you be interested in being consulted again as negotiations unfold? (checking "no" here does not exclude you from future engagement, should you wish to reengage)

Yes

Official Information Act 1982

14 If you think there is a reason why anything in your submission should not be made public, please let us know here.

OIA:

15 If you are an individual, as opposed to an organisation, we will consider removing your personal details from the submission in the event of a request under the OIA. Are you happy for your personal information to be released?

Yes

Released under the Official Information Act 1982