MINISTRY OF JUSTICE
Tāhū o te Ture

DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

New Zealand accession to the Budapest Convention on Cybercrime

Summary of submissions on the July 2020 consultation paper | December 2020

New Zealand Government

Contents

Introduction & summary

What we consulted on

In July 2020 the Department of the Prime Minister and Cabinet and the Ministry of Justice released a consultation paper to invite public feedback on a proposal to join the Council of Europe Convention on Cybercrime (the Budapest Convention). The paper outlined what the Budapest Convention is, the advantages and disadvantages of accession, the legislative implications, and possible costs.

Part of the consultation paper outlined the proposal for a data preservation scheme, which would be one of the legislative implications of accession to the Budapest Convention. Views were sought on the advantages, implications, and costs of joining, any considerations for implementation, and, taking all factors into account, whether New Zealand should accede to the Budapest Convention.

The specific proposals of the consultation paper are outlined in each of the themes set out below. Information on the decisions made by Cabinet regarding accession and implementation which were informed by submissions can be found on the Ministry of Justice website.

Submissions received

The submission process closed in late September 2020. A total of 17 submissions were received from a range of private sector companies, organisations, and individuals. The names of individual submitters have been withheld to protect their personal information. The names of the 13 organisations that submitted are below:

- Te Hunga Rōia Māori o Aotearoa/The Māori Law Society (THRMOA)
- Interim Māori Spectrum Commission (IMSC)
- Mega Limited (MEGA)
- Internet NZ
- Telecommunications Forum (TCF)
- Spark
- Microsoft
- PaloAlto Networks
- Copyright Licensing Limited
- NZ Authors
- ANZ Screen Association
- WeCreate
- Office of the Privacy Commissioner (OPC)

In addition to formal submissions, engagement was undertaken with several Māori groups and individuals with an interest in this subject area.

What we heard – summary

The majority of submitters supported accession to the Budapest Convention. Submitters acknowledged that accession would be a benefit to New Zealand in addressing international crime, as well as protecting copyright.[1]

Many of the submissions focused on the proposed data preservation scheme. The feedback on the scheme covered the implementation of the scheme and associated costs, the impact of preservation orders on digital privacy rights, and potential safeguards and other ways to improve transparency.

Māori groups and individuals that we heard from did not feel that they had sufficient confidence at this stage to support accession.[2] Some felt that further and broader engagement was needed before a decision was made. Feedback included concerns that international interests may be put ahead of the Crown's Treaty of Waitangi obligations, that accession could exacerbate the overrepresentation of Māori in the criminal justice system, and concerns about the protection of Māori data. To mitigate these risks, some submitters suggested a role for Māori in governance and oversight, while some suggested a process for Māori to challenge data preservation requests. Many of the submissions from Māori groups and individuals raised issues much broader than those related to the changes to legislation which have been proposed and speak to the relationship between Māori and the Crown in the criminal justice system.

Themes of submissions

Benefits and advantages of accession

Submitters from the telecommunications and cloud storage sector recognised that the Budapest Convention is an important step to fight cybercrime and ensure that law enforcement agencies can effectively respond to cybercrime, especially given its transnational nature. Microsoft stated that the risks of not acceding are likely to be greater than the risks of acceding, because staying outside of the Budapest Convention's international cooperation framework may impede New Zealand's ability to effectively combat cybercrime.

Internet NZ supported accession because the Budapest Convention enables information sharing to address cybercrime in a way that is based in legal due process. Their submission also noted the benefit of becoming part of international conversations to address cybercrime and being a voice for a rules-based international order.

The submission from PaloAlto Networks noted that the Budapest Convention is a "valuable mechanism" and it will make it easier to co-operate with other member countries. This submission also noted the benefit of the 24/7 network which provides national contact

[1] Article 10 of the Convention requires countries to criminalise the intentional breach of copyright on a commercial scale. New Zealand law already complies with this requirement.

[2] Any submission indicating that it was being provided from a Māori perspective, or by an individual or organisation identifying as Māori has been considered as a Māori submission

points to coordinate investigations and requests for information, and the importance of accession in light of several recent cyber incidents in New Zealand.

The four submissions received from organisations involved in the creative community supported accession because the Budapest Convention criminalises copyright infringement by means of a computer system. Individual submitters supported accession because cybercrime and cyber-enabled crime are an international problem which requires an international response, and because accession would facilitate international relationships.

MEGA noted that accession to the Budapest Convention is 'long overdue' and offered support for submission as long as concerns about the implementation of the data preservation scheme are addressed.

THRMOA agreed in principle with the "reason for accession being to assist New Zealand law enforcement agencies to better identify, respond to, and prevent cybercrime in New Zealand, leading to a safer digital environment overall". However, THRMOA did not support accession at this time due to other concerns which are outlined in the themes below.

The OPC and one individual submitter did not offer any comments on accession but focused on the legislative changes required for accession. These are addressed below.

Data preservation scheme

One of the legislative changes required for accession is the introduction of data preservation orders into the Search and Surveillance Act 2012. Many of the submissions focused on the elements of the data preservation scheme as proposed in the consultation paper and accompanying factsheets.

Conditions of a data preservation order

What was proposed

The consultation paper outlined a proposed scheme which was based on the recommendations made by the Law Commission in its 2017 report on the Search and Surveillance Act 2012, which proposed that a tightly constrained preservation scheme be implemented. The consultation paper stated that the proposed conditions for an order to be issued would be that an order can only be issued if the decision-maker is satisfied that:

- The relevant enforcement agency intends to apply for a production order in respect of the identified data; and
- The issuing officer is satisfied that the requirements for obtaining a production order, including under section 72 of the Search and Surveillance Act, are likely to be met in the circumstances of the case; and
- Preservation is necessary because the data is vulnerable to loss or modification.

Because the threshold for preservation is aligned with that of a production order, the consultation paper stated that preservation orders are unlikely to be frequently used in support of domestic law enforcement investigations (since generally it would make more sense to seek a production order for the information, in a single step).

What submitters told us

The five submitters who commented on the conditions for data preservation orders all supported a tightly constrained scheme where the conditions matched those of a production order.

MEGA's submission said that there is a risk preservation orders are perceived as easier to obtain than production orders and may be used to buy time before adequate proof has been obtained to justify a production order. This would result in an increase of orders. Spark's submission stated that "we are supportive of a regime where a preservation order is effectively just asking us to run a production order on data that would otherwise be modified or lost ahead of a formal request, and to store this data for a longer period than we would under our usual business rules". The OPC also recommended that the conditions for a preservation order align with those of a production order. Internet NZ supported the approach to data preservation, stating they would oppose "a more general legal requirement for data retention by organisations, due to the negative impacts this would have on privacy, security, and trust, which we think would be out of step with community expectations in New Zealand".

Reasons for aligning the conditions of preservation and production orders were varied among submitters. Some submitters were concerned that a difference in conditions would result in increased cost and have impacts on the practicality of the scheme. Others were concerned that the scheme for data preservation should be as limited as possible to limit the impact on digital privacy rights.

Two of the submitters recommended that the words "likely to be met" should not be used in the conditions for the order, rather the conditions should be that the grounds of a production order "are met", or there is a reasonably held belief that they "will be met".

In addition to the feedback on the conditions of a data preservation order, some submitters expressly stated that the scheme should only be available to overseas agencies. Spark qualified this sentiment by stating that domestic agencies should only have access to preservation orders if there is the ability to charge that agency for cost recovery.

Furthermore, TCF submitted that preservation orders should only be available for the crimes outlined in Articles 2-10 of the Budapest Convention, rather than "an offence" as outlined in section 72 of the Search and Surveillance Act 2012 (i.e. a criminal offence punishable by imprisonment). MEGA's submission outlined a risk that there is a different definition of crimes between countries, so a preservation order request may be submitted for evidence of a crime which is not an offence in New Zealand. MEGA's view was that actioning foreign preservation orders for acts that are not crimes in New Zealand may impact on human rights if the request is used for political purposes.

Safeguards – who makes the order & how

What was proposed

Two elements of the proposed data preservation scheme dealt with who can issue the order, and how it is issued. The consultation paper proposed that the statutory power to make a

preservation order would sit with the chief executive of the agencies empowered to seek the orders (and could be delegated to suitably qualified and responsible officials).

The consultation paper also listed the agencies who would be empowered to apply for preservation orders, based on the agencies in the Search and Surveillance Act who have the ability to apply for production orders. For international requests, the consultation paper stated that it is still being considered whether all agencies with domestic preservation order powers would be empowered to receive and action incoming foreign requests or only a subset of those agencies.

Regarding how the order is issued, the consultation paper also outlined the circumstances in which a verbal order could be made.

What we heard

Of the submitters who commented on these elements of the data preservation order scheme, two submitters disagreed with the ability for Chief Executives to delegate the power to issue an order, stating that it should remain with the Chief Executive of the agency. Three other submitters stated that the power to issue a preservation order more appropriately sits with the judiciary because it is a power which impacts New Zealanders' privacy rights.

Regarding the agencies empowered to use preservation orders, Spark suggested that industry be given clarity on which agencies can request preservation orders so that operators can confirm the validity of requests. One submitter stated that international requests should only be authorised by the NZ Police and the "Central Authority", rather than all the domestic agencies with power to apply for production orders.[3] This feedback was similarly provided by Spark, who submitted that only some of the domestic agencies should be able to action requests from international parties. In Spark's view this would "also help with monitoring volumes of international preservation requests and ensuring consistency of approach."

There was strong opposition to the proposed use of verbal orders. Some submitters highlighted the practical challenges of actioning a verbal request when the subject matter is quite technical and could easily be misunderstood or miscommunicated. For example, MEGA's submission said that a complex URL could be 50-150 characters long, and one transposed character will obtain a completely different dataset.

Submissions also highlighted the risk that there will be differences between a verbal order and what is subsequently communicated in writing, creating administrative burdens and unnecessary complications. Concern was expressed that verbal orders would be difficult to track and audit later, which would restrict transparency and create issues if the order is later challenged. The IMSC submission also touched on "transparent, robust and unambiguous processes [that] include written requests".[4]

[3] "Central Authority" refers to the Attorney-General of New Zealand, who is responsible for reviewing and approving mutual legal assistance requests.

[4] Interim Māori Spectrum Commission (2020). *Position statement on the Budapest Convention on Cybercrime.* Auckland, Aotearoa/New Zealand. The IMSC requested that their work be cited in the summary of submissions. Any reference to the IMSC in the following refers to this same document.

Finally, Spark opposed verbal orders because they thought verbal requests for a preservation order would be issued 'just in case' and then later on the agency would decide that is actually not needed, or the conditions for a preservation order are not met.

Appeals, guidance and reporting

What was proposed

If the recipient of the preservation order believes the data subject to the order would be unreasonably onerous or resource-intensive to preserve, or that there is some defect in the application for an order, there would be a mechanism for appeal and resolution.

The consultation paper stated that guidance would be developed for agencies applying for a preservation order, for recipients of preservation orders, and for international countries who request preservation orders. It also set out that parliamentary reporting would be required of any agency who made more than 100 preservation orders per annum.

What we heard

Submitters were supportive of an appeal mechanism. One submitter suggested strengthening the appeal mechanism to refuse overseas orders where they are for an action that is not considered a crime in New Zealand, and MEGA's submission suggested additional grounds for appeal such as "factually inaccurate" or "inappropriate political motives". MEGA's submission also provided detailed comments about how the mechanism should work.

The submission from THRMOA stated "that there should be a clearer process for Māori to challenge data preservation orders. For example, a committee with quasi-judicial functions could decide if an order was lawful or prejudicial to the Government's Te Tiriti obligations."

The IMSC submission stated that "if the IMSC or its ISP customer/user chooses to legally challenge a 'data preservation order' in Courts, there needs to be further discussion towards who should pay costs".

Guidance for agencies who can issue preservation orders was supported by MEGA. The IMSC suggested that "the Government provide annual workshops for Māori data holders on their obligations and options". Spark's submission requested specific guidance on how to handle consumer personal data requests when a preservation order has been enacted on the customer's account.[5]

Multiple submitters also expressed support for reporting obligations on agencies who use the preservation order power. Rather than the threshold of 100 per annum as suggested in the consultation paper, submitters recommended that every agency report on all preservation orders made. One submitter also suggested reporting on preservation orders that lapsed or were revoked without further action, as well as the number of foreign requests for preservation orders that were refused.

[5] This relates to confidentiality orders – see below.

Costs & cost recovery

What was proposed

The consultation paper estimated between 10 and 15 preservation orders will be issued in New Zealand annually, based on the current mutual assistance cases each year that involve a request for preservation of information. Based on previous consultation with telecommunications companies the cost of responding to a preservation order was estimated at $1,000, which involves time and resources spent on receiving and checking an order, processing capacity to copy and store the data, and other associated costs.

What we heard

Feedback about the cost of a data preservation scheme was mixed. Microsoft's submissions stated that "the costs associated with data preservation order compliance are marginal given the low cost of data storage itself… certain costs primarily arise from the robust process of assessment of the data preservation orders themselves by the recipient but we consider the existence of such a process to be already an industry standard among cloud service providers".

MEGA's submission took the view that the costs of data preservation may not be as great as $1,000. MEGA already assists law enforcement and other government agencies with data preservation on a voluntary basis and said that this is "not overly onerous". However, MEGA's view is that if the data preservation order scheme is complicated or uncertain, this would alter the costs associated with an order. In addition, MEGA noted that there may be costs associated with any appeals over preservation orders, and this factor should be part of any consideration of the appeals process (see feedback above).

TCF and Spark both submitted that the estimated 10-15 preservation orders per year and $15,000 total cost is too low. Both submitters were of the opinion that once preservation orders are available for use, usage will increase beyond this estimate. Each submission outlined the way in which the costs for complying with preservation order requests could go beyond the estimate in the consultation paper – because of the complexity of requests, or because of the resources required to comply with an order.

TCF and Spark refuted the view expressed in the consultation paper that because a voluntary scheme exists currently, there is consequently a justification for mandating data preservation without cost-recovery. TCF's submission stated that "companies must have the ability to recover their costs", and Spark's submission said that "as a matter of principle, commercial organisations should not be mandated to provide services to government for free". Concern was expressed that lack of cost-recovery may result in providers being swamped in requests, or law enforcement agencies submitting frivolous requests, or requests where the data which is preserved is more than what ultimately is required by a production order. A cost-recovery scheme was supported by both submitters, and Spark provided further details about what such a scheme could look like.

One individual submitter also reflected the concerns about cost, stating that "the estimated cost of responding to a data preservation order of $1,000 is unreasonably large for small businesses… [the Government] should establish a fund to defray the cost of such orders". The IMSC also stated that "the cost burden of compliance on IMSC and its users" should be met by government.

Duration of order

What was proposed

The consultation paper proposed that once issued, a preservation order would be 30 days for domestic orders, or 180 days for foreign orders. It also stated that the orders can be extended indefinitely, at each extension for a period not exceeding 30 days (domestic) and 180 days (foreign) if they meet certain criteria. Finally, the proposal stated that if the grounds for the order no longer exist, or the investigation is discontinued, the agency must serve notice discontinuing the order. Following a time period lapse or discontinuation, the data would revert to its normal state (i.e. subject to the normal Privacy Act requirements and can be deleted in the normal course of business).

What we heard

Submitters' views on the duration varied, although all who touched on this topic agreed that orders should not be able to be extended indefinitely. Spark and TCF accepted the timeframes for both domestic and foreign orders, while MEGA and an individual submitter stated that the duration of domestic orders should be 20 days (in line with a recommendation by the Law Commission), and the same individual's submission stated that the duration of foreign orders should be between 60 and 90 days, not 180 days.

The ability to extend orders an indefinite amount of times was not supported by all the submitters who mentioned it. Some supported a maximum number of extensions, while others supported a maximum time period up to which point orders could be extended.

The OPC and one individual submitter all encouraged a requirement for data to be proactively destroyed once a preservation order lapses or is discontinued to avoid the risk that data is inadvertently and inappropriately retained.

Remaining elements of data preservation scheme

There were a few elements of the proposed data preservation scheme that were only addressed by one or two submitters.

TCF submitted on penalties, asking for clarity that a penalty would not apply if the loss of data was due to a third party – i.e. when multiple parties have control over data because it is stored in the cloud. An individual submitter stated that the proposed penalties are higher than those for other serious offences, and requested further information about the justification for this proposal.

The consultation paper confirmed that preservation orders would not be able to be used prospectively, and no specific formatting requirements for the data. This was supported by Spark and TCF.

Finally, the consultation paper outlined that there would be an enabling provision for Article 17 of the Budapest Convention which addresses the release of traffic data in order to identify the path through which a communication has travelled. The only submission on this was from MEGA, who outlined their concern that this would act as a quasi-production order and potentially identify users without the burden of meeting the production order threshold. MEGA's submission proposes criteria that would need to be satisfied before the traffic data is released under a preservation order.

Other feedback related to data preservation

There were some comments from MEGA which touched on concerns about the data preservation scheme beyond what was proposed in the consultation paper. These involved the need for safe harbour provisions, and the creation of a formal process which may deter overseas agencies from working directly with the companies who hold the data in the first place.

Regarding safe harbour provisions, MEGA's submission made the point that once a data holder is made aware of objectionable or illegal material, they are required to follow a certain process to take it down or delete it in order to avoid liability. Because the data preservation order will notify data holders of the existence of the material, and require it to be preserved, MEGA's view was that safe harbour provisions are necessary so that data holders are able not liable for holding the material.

The second concern that MEGA raised about the data preservation scheme was that the existence of a formal process for overseas countries to request data preservation, this will stop them working informally with the data holders in the first instance. MEGA states that in urgent cases with objectionable or extreme content, they do not require a formal order, but co-operate to preserve data and block access. Rather than replacing this, MEGA indicated that they would like this informal co-operation to continue either by itself or in addition to a formal request for a data preservation order or the mutual legal assistance process.

Other legislative changes proposed

What was proposed

Besides the data preservation scheme, the consultation paper proposed legislative changes to add third party confidentiality orders to the Search and Surveillance Act 2012, changes to the Mutual Assistance in Criminal Matters Act 1992 (MACMA), and proposed one reservation to the Budapest Convention.

Third party confidentiality orders would require third parties who are aware of the execution of a surveillance device warrant or preservation order to keep this confidential. This would only take effect while the investigation is taking place, and only if the investigation were to be jeopardised by the disclosure of the order.

Surveillance device warrants are already available for domestic criminal investigations but would be added to MACMA so that they could be used in New Zealand to obtain information relevant to overseas investigations and vice versa. This would be an incremental extension of assistance already available through mutual assistance provisions. Another

proposed change to the mutual assistance legislation is the ability to delay notifying a party affected by a search warrant if, for example, it would jeopardise an ongoing investigation. While the latter change is not strictly required for accession, it directly influences the effectiveness of the mutual assistance New Zealand provides.

The consultation paper also proposed invoking one reservation to Article 22(1)(d) of the Budapest Convention, which requires parties to establish jurisdiction over their citizens if they commit a Budapest Convention offence, regardless of where the crime was committed. New Zealand already has existing provisions for extraterritorial jurisdiction in the Crimes Act 1961, so may join several other countries in invoking a reservation to this article.

What we heard – confidentiality orders
On confidentiality, the OPC submitted that these could be added to the legislation in such a way as to complement the Privacy Act. Under the Privacy Act regime, an agency responding to a request for personal information must either provide the information or apply one of the available withholding grounds. In the view of the OPC, confidentiality orders could be dealt with under one of these withholding grounds. The OPC also recommended requiring agencies to notify affected individuals either at the conclusion of an investigation or the expiry of a preservation order (unless this would prejudice the maintenance of the law).

Spark's submission also touched on confidentiality orders and requested guidance about how to deal with personal data requests when there is a preservation order on the account that is confidential. Spark suggested that there should be a statutory exemption so that upon a request for personal data, data holders should only provide data that they would hold as part of business-as-usual, and not that which may be being held because of a preservation order.

What we heard – changes to MACMA
Two submitters touched on the proposed changes to MACMA. The OPC noted the proposed changes, requested further information about delayed notification and how this is dealt with in current processes, and noted that Crown Law's involvement in the mutual assistance process is an important safeguard for the mutual legal assistance process.

The second submitter opposed the changes to MACMA, instead saying that New Zealand should progress a draft Mutual Legal Assistance bill which was developed by the Law Commission in 2016. This submitter noted that although they did not oppose the addition of surveillance device warrants to MACMA, these would be better considered as part of changes to the whole of MACMA, rather than in isolation. In contrast, this submitter strongly opposed the addition of delayed notification provisions because it has the potential to undermine digital privacy rights of affected persons. In this submitter's view, the proposed change is not a minor amendment, and should only be progressed as part of a mutual legal assistance reform where this kind of provision could be "drafted and applied in a manner that is expressly sensitive to, and protective of, the underlying digital privacy rights of affected persons, whether these are New Zealanders or others".

What we heard – Reservations
The only submitter to touch on the proposed reservations to the Budapest Convention was

MEGA. MEGA's submission noted that reservations to Article 22(1)(d) have been sought by other countries for a range of reasons, as well as reservations to other articles of the Budapest Convention. MEGA's submission took the view that more information is needed as to why a reservation is necessary for Article 22(1)(d), as well as further consideration of whether any other reservations are required.

Feedback on other articles of the Budapest Convention

Although not expressly raised by the consultation paper, some submitters referred to and offered feedback on other articles of the Budapest Convention. MEGA's submission raised potential issues with Article 24 of the Budapest Convention which deems cybercrime offences as extraditable offences. In MEGA's view, this article should be considered very carefully alongside New Zealand's existing extradition treaties to avoid the risk of "unjust treatment of New Zealand citizens and residents".

The submission from THRMOA raises concerns about Articles 10, 26 and 27:

a) Article 10 concerns offences relating to infringements of copyright and related rights. It requires member countries to establish the criminal offences outlined by a variety of other international treaties. THRMOA expressed concern that as New Zealand is not party to the Rome Convention, accession would equate to automatic accession to the Rome Convention, without specific consultation on that treaty.
b) Article 26 allows member countries to forward information obtained as part of its own investigations to another member country, within the limits of its domestic law, and without prior request. THRMOA's concerns relate to the potential reach of this article, particularly concerning Māori data. In addition, they express concerns that relate to the purpose for which this article can be used, saying that it should not be used to subvert the mutual assistance process, and use of this article should require Parliamentary reporting.
c) Article 27 allows a member country to refuse assistance based on a few grounds – including if the execution of the request is likely to prejudice its sovereignty, security, *ordre public*, or other essential interest. THRMOA's submission seeks clarification of whether Te Tiriti o Waitangi/Treaty of Waitangi is an "essential interest" on the basis of which a request could be refused.

Feedback regarding Māori data

Concerns were raised by several submitters about the use and protection of Māori data. THRMOA said that "Māori must have sovereignty over Māori data, and Māori only should determine how, and what, data is shared". This concern were echoed by the IMSC who want assurance that "wide-sweep data harvesting on Māori communities or groups is not allowed, and data requests that target Māori 'by stealth' are exposed and managed with Māori" and that "international geo-political ambitions are rejected by the NZ Government where they could impact Māori".

Two suggestions for addressing the above concerns were to include a Te Tiriti o Waitangi/Treaty of Waitangi provision or clause into New Zealand's accession, or into the legislation, and establishing a governance or oversight role for Māori.

The purpose of including a clause referencing Te Tiriti o Waitangi/Treaty of Waitangi according to submitters would be to indicate its "important constitutional role", to recognise that "Māori data is a taonga", and to provide a basis upon which to refuse requests for assistance that deal with Māori data.

The proposal to establish a governance or oversight role for Māori took several forms. One submitter recommended a specialised Māori data governance group be established to advise law enforcement agencies on the best way to deal with Māori data. This was echoed by the submission from the IMSC which recommended that the New Zealand government "establish a skilled and resourced Māori Governance group to provide oversight to the Budapest Convention", and "partner with the IMSC for a specialist Māori 'on-call' role, to determine the relevance to Māori of any data related requests as they are received, and to work with the Government to manage its Māori response and communications strategy".

THRMOA also noted that there should be a process for Māori to challenge data preservation orders, as noted above. Their submission also recommended that Māori be included in annual reporting as well as any reviews of the convention.

Consultation and engagement

What was proposed

The consultation paper outlined a number of further opportunities to engage in the process, if the Government decides to proceed with acceding to the Budapest Convention. This includes the Select Committee process as part of the parliamentary treaty examination, consultation as part of the implementation process as required, and the Select Committee process as part of the examination of any bill to implement the legislation.

What we heard

The OPC's submission noted that it is unclear what Māori organisations and groups have been engaged in consultation, and that this is critical to understand the impacts of accession. This sentiment was echoed by an individual submitter as well. THRMOA expressed concerns in their submission about the length of time that was given for submissions, about the adequacy of consultation (including whether research has been conducted into the impact of the Budapest Convention on indigenous peoples in nations that have already acceded), and about the validity of the consultation (because the Government already made an in principle decision to accede).

The TCF submission also noted that they expect further consultation with the telecommunications sector, to verify the assumptions underpinning, and costs associated with the data preservation scheme.

Concerns about the impact of the Budapest Convention as a whole

Unease was expressed by Māori submitters about accession to the Budapest Convention because of the fear that international interests may be put ahead of Te Tiriti o Waitangi/Treaty of Waitangi when considering mutual assistance or data preservation requests. THRMOA recommended that the Government comprehensively assess its obligations under Te Tiriti and ensure they are not inconsistent with those imposed by the

Budapest Convention, and if there is any inconsistency to address this prior to accession, rather than afterwards.

THRMOA was also concerned that accession might further exacerbate the overrepresentation of Māori in the criminal justice system because "the systemic bias that exists in the criminal justice system is likely to result in disproportionate criminalisation of Māori as cybercriminals". Their submission stated "we remain concerned there will be little difference in practice with how Police operate in the digital environment compared to the current criminal justice system".

Comments about 2nd Additional Protocol; CLOUD Act agreement/other work

The Budapest Convention currently has one Additional Protocol which addresses xenophobia and racism. There is a Second Additional Protocol under negotiation which seeks to make the mutual legal assistance process timelier, and address other issues. These Protocols would be subject to a separate accession process, should New Zealand wish to join them. Nevertheless, several submitters touched on these as well as on the potential for a CLOUD Act agreement with the United States, which would also be subject to a separate decision process, should Ministers decide to seek suck an agreement.[6]

Two submitters expressed support for a CLOUD Act agreement, while one submitter opposed it. One submitter expressed support for the Additional Protocol on Xenophobia and Racism, while two noted that more consultation would be necessary before joining either of the Additional Protocols.

On further work that should be undertaken, the submission from PaloAlto Networks encouraged New Zealand to update its National Plan to Address Cybercrime 2015, to work with regional partners to build capacity to address cybercrime, and to promote voluntary sharing of cyberthreat information between public and private partners. The submission from Internet NZ also noted that it is important to link international developments and domestic policy goals.

[6] The Clarifying Lawful Overseas Use of Data Act was introduced to deal with issues raised in Microsoft Corp v United States where Microsoft argued it was not able to release information on a US citizen held on one of Microsoft's servers in Ireland.