



15 September 2020



Reference: OIA-2019/20-0582

Dear 

**Official Information Act request relating to the Budapest Convention on Cybercrime**

I refer to your request made under the Official Information Act 1982 (the Act), received as a partial transfer from the Ministry of Justice on 17 June 2020. The part transferred to the Department of the Prime Minister and Cabinet (DPMC) asked for:

*“The NZ government's plans to accede to the Budapest Convention on Cybercrime”*

I note the time frame for responding to your request was extended by DPMC on 15 July 2020 under section 15A of the Act by 30 working days, in order to allow further consultations to be undertaken before a decision could be made on your request. I further note that this letter of 15 July 2020 refused your request insofar as it relates to Cabinet paper “Budapest Convention on Cybercrime: Approval to Initiate the First Stage Towards Accession” and the related Cabinet minutes under section 18(d) of the Act, as this information is, or will soon be, publicly available on DPMC's website.

I have taken your request to be for Cabinet Papers, Aides Memoire and Briefings related to New Zealand's plans to accede to the Budapest Convention on Cybercrime. The following items have been identified as in scope. This material includes two items prepared by the Ministry of Justice for inclusion in DPMC's response to your request.

Item	Date	Document Description/Subject	Prepared by
1.	20 February 2018	Aide Memoire: Council of Europe Convention on Cybercrime (Budapest Convention)	DPMC
2.	9 October 2018	Briefing: Budapest Convention accession – opportunities & analysis	DPMC and MoJ
3.	22 November 2018	Aide-Memoire: Release of Data Preservation Consultation Paper	DPMC
4.	7 December 2018	Aide-Memoire: Follow-up: Release of Data Preservation Consultation Paper	DPMC
5.	March 2019	Data Preservation Consultation Paper	DPMC and MBIE
6.	27 November 2019	Briefing: Budapest Convention: Legislation Bid	DPMC

7.	9 December 2019	Briefing: Targeted Engagement on Accession to the Budapest Convention	DPMC and MoJ
8.	19 February 2020	Briefing: Options for Cabinet Consideration of Accession to the Budapest Convention	DPMC
9.	11 March 2020	Briefing: Cabinet Paper: In-Principle Decision on Accession to the Budapest Convention	DPMC
10.	12 March 2020	Aide-Memoire: Accession to the Budapest Convention - Cabinet paper	MoJ
11.	20 May 2020	Aide-Memoire: Accession to the Budapest Convention – Cabinet paper	MoJ
12.	22 May 2020	Aide-Memoire: Social Wellbeing Committee Discussion on Accession to the Budapest Convention on Cybercrime: Speaking Points	DPMC
13.	28 May 2020	Budapest Convention: Timeline for Engagement and Final Decisions on Accession	DPMC

Some information has been withheld in these documents under the following sections of the Act:

- 6(a), to protect the security or defence of New Zealand or the international relations of the Government of New Zealand,
- 6(b), to protect the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government, or by any international organisation,
- 9(2)(a), to protect the privacy of individuals,
- 9(2)(b)(ii), to protect the commercial position of the person who supplied the information, or who is the subject of the information,
- 9(2)(ba)(i), to protect the supply of similar information in the future,
- 9(2)(f)(iv), to maintain the confidentiality of advice tendered by or to Ministers and officials,
- 9(2)(g)(i), to maintain the effective conduct of public affairs through the free and frank expression of opinion, and
- 9(2)(h), to maintain legal professional privilege.

In addition to this, a briefing prepared by DPMC has been withheld in full under sections 6(a), 6(b), 9(2)(ba)(i), 9(2)(f)(iv), 9(2)(g)(i) and 9(2)(j) of the Act.

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 DPMC'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



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



DEPARTMENT of the  
PRIME MINISTER and CABINET

*Te Tari o Te Pirimia me Te Komiti Matua*

# Aide-memoire

Minister of Broadcasting, Communications and Digital Media

(Hon Clare Curran)

**From:** Paul Ash

**Date:** 20 February 2018

**Security Level:** Restricted

**Report No:** DPMC-2017/18-647

## Council of Europe Convention on Cybercrime (Budapest Convention)

### Purpose

1. To provide background on the Council of Europe Convention on Cybercrime 2001 (known as the Budapest Convention) and the measures required to bring New Zealand's laws and investigative processes in line with the Convention.

### Background

2. During our discussion on 12 February about the Cabinet paper on the review of New Zealand's Cyber Security Strategy and Action Plan, you asked for more information about the Budapest Convention and what is required to enable New Zealand accession.
3. Accession to the Budapest Convention is an action in the existing Action Plan and National Plan to Address Cybercrime, and it was also included in the 2011 Cyber Security Strategy. Cabinet agreed in December 2012 that work to accede to the Budapest Convention should be carried out in accordance with the timeframe provided by the Minister of Justice.
4. 9(2)(g)(i)

The focus of government work in this area was placed on the Telecommunications (Interception and Security) Act 2013, the Government Communications Security Bureau Act 2013, and, subsequently, on the Intelligence and Security Act 2017.

5. In addition to these factors, competing priorities also made it challenging for the Ministry of Justice to progress work on the Convention. In 2016 the question of a data preservation regime sufficient to enable accession to the Convention was included as part of the Law Commission review of the Search and Surveillance Act



2012, which has now been completed. Work led by NCPO and the Ministry of Justice is now underway.

6. 9(2)(g)(i)

The Ministry of Justice is responsible for administration of most of the legislation that would require amendment to enable accession to the Convention (for example, the Crimes Act, Mutual Assistance legislation, and Search and Surveillance Act).

## What is the Budapest Convention?

7. The Budapest Convention is the first international agreement on **cybercrime**. The trans-national nature of cybercrime, with perpetrators often based overseas and highly organised, makes it difficult for law enforcement agencies to access evidence and pursue investigations. The Convention, by **standardising offences** and improving processes for accessing information in different jurisdictions, assists law enforcement agencies to investigate and respond to cybercrime.
8. The Council of Europe, based in Strasbourg, includes 47 European countries. It was set up to promote democracy and protect human rights and the rule of law in Europe. Despite its Council of Europe origins, the Convention is open to accession by non-European countries. A total of 56 countries have acceded as of February 2018. This includes 43 of the 47 Council of Europe members and 13 non-members of the Council of Europe, including Tonga in 2017, and Australia, UK, US Canada and Japan, among New Zealand's closest partners. See Attachment A for a list of parties to the Convention.
9. The Convention sets out a number of measures to be adopted by parties to the Convention to improve international responses to cybercrime.
10. In order to **standardise national laws relating to cybercrime offences**, parties must ensure the following offences are covered in their domestic laws:
  - i. offences against the confidentiality, integrity and availability of computer data and systems (e.g. illegal access to computer systems, illegal interception of computer data, interference with computer data, interference with the functioning of computer systems, and misuse of computer devices);
  - ii. computer-related offences such as fraud or forgery;
  - iii. content-related offences such as the distribution of child pornography through computer systems; and
  - iv. offences related to infringements of copyright and theft of intellectual property.
11. The Convention requires parties to adopt certain **powers and procedures for investigating cybercrime offences**, consistent with domestic and international

human rights obligations and other safeguards. The powers and procedures include:

- i. measures to order the expeditious *preservation* of computer data and computer traffic data for up to 90 days;
- ii. measures to order the production of specified computer data and subscriber information (Production Orders);
- iii. measures to enable search and seizure of stored computer data;
- iv. measures to collect computer *traffic* data associated with specified communications in real time; and
- v. in relation to serious offences, measures to collect computer *content* data in real time.

12. The Convention sets out a number of principles and procedures related to **international cooperation amongst the parties on investigating cybercrime.**

This includes:

- i. deeming the cybercrime offences listed in paragraph 10 above as extraditable offences;
- ii. procedures relating to mutual assistance and sharing of information in the investigation of cybercrime offences;
- iii. provisions for mutual assistance between parties on expeditious *preservation* of computer data and computer traffic data, and access to computer data and computer traffic data; and
- iv. the establishment of a 24 hour/7 day a week designated point of contact to ensure the provision of assistance between parties for the investigation of cybercrime.

## How do states accede to the Budapest Convention?

13. In order to accede, a state must formally express interest. If the parties to the Convention agree, the state is invited to participate as an observer at Budapest Convention Committee meetings and is on a five year "on-ramp" to complete the procedures necessary for accession.


14. A decision on whether New Zealand should formally express interest in acceding to the Convention would need to be made by Cabinet. Any Cabinet paper would be accompanied by a National Interest Analysis, which would set out the advantages and disadvantages of becoming a party to the Convention. If Cabinet approved, the National Interest Analysis would be presented to the House of Representatives. A select committee would then consider the Convention and National Interest Analysis and have 15 sitting days to report back to the House with recommendations. The Government must then table a response to any recommendations within 90 days.




15. During the five year “on-ramp” period, New Zealand would need to undertake legislative amendments and some operational changes to complete the procedures necessary for accession.

### **Why should New Zealand accede to the Budapest Convention?**

16. There are three broad reasons for New Zealand to accede:
- a. It would allow NZ Police and other agencies to better access information relevant to cybercrime investigations.
  - b. It would demonstrate New Zealand’s support for the most prominent international instrument addressing computer crime and signal our commitment to international cooperation in this area.
  - c. It would enable New Zealand to contribute to emerging international law and procedures on cybercrime issues. For example, parties to the Convention are currently developing a Protocol to the Convention relating to access to evidence in the cloud.

17. 6(a), 6(c)
- 

### **Active international efforts to encourage New Zealand accession**

18. 6(a), 6(b)
- 

19. At an Intergovernmental Expert Group meeting on cybercrime in Vienna, April 2017, in addition to the Head of the Cybercrime Division within the Council of Europe, 6(a) all invited New Zealand to participate as an observer at the next meeting of the Budapest Convention Committee of the Council of Europe. The Committee meetings are attended by parties to the Convention, observer states on the “on-ramp” and a number of international organisations such as Interpol, Europol, and the African Union etc.

20. Accordingly, a senior official from the Ministry of Justice attended the Budapest Convention Committee meeting in June 2017. He affirmed the value of the Convention for cross-border cybercrime investigation, particularly for improved

data flow between states, and the benefits of engagement with parties to the Convention.

## **What does New Zealand have to do to accede to the Convention?**

21. New Zealand's cybercrime offences (under the Crimes Act; Film, Video, Publications Classification Act; Copyright Act) are broadly consistent with those set out in the Convention (paragraph 10). Some minor amendments to the Crimes Act may be required (and Ministry of Justice will consider this in the context of a broader review of the Act this year).

### ***Data preservation orders***

22. The main barrier to our accession is a lack of a 'data preservation' scheme in New Zealand. There is currently no obligation (and often no business reason) for communication providers or other information holders to store data which might play a vital role in law enforcement. The data is often deleted within hours or days of its creation.
23. A data preservation scheme would enable law enforcement to issue an order to communication providers or other information holders to preserve relevant data for up to 90 days. This would prevent the data being deleted whilst relevant agencies seek a production order (under the Search and Surveillance Act 2012) requiring the data to be handed over.
24. The January 2018 joint report of the Law Commission and Ministry of Justice on the review of the Search and Surveillance Act 2012 ("S&S Act") recommended that the government consider accession to the Budapest Convention, including the establishment of a "tightly constrained" data preservation regime under this Act.
25. In considering a data preservation scheme, there will need to be engagement with communication providers or other information holders as there will be technical and, possibly, financial implications related to the requirement to preserve data when required by law enforcement.

### ***Data preservation vs data retention***

26. It is important to note that data preservation is different to data retention. Data preservation orders are issued for specific data (usually call associated data or metadata *and* content) in a discrete case. Data retention is the requirement that communication providers or other information holders retain metadata or call associated data (but not content) for a certain period of time in case it is required by law enforcement.
27. Data retention enables relevant agencies to access older, but more limited metadata which is often relevant to an investigation; whereas data preservation enables relevant agencies to access much fuller data (both content and metadata) for a specific investigation. But because communication providers or



other information holders might not make a practice of storing data, it may not be possible through data preservation to access historical content and metadata, which is often more useful to an investigation.

28. Both Australia and the United Kingdom have data retention schemes. Australia introduced data preservation in 2012 to enable it to accede to the Budapest Convention and subsequently introduced a data retention scheme, which came into effect in April 2017. Australia requires metadata (not content) to be stored for two years and has agreed to contribute \$128.4 million over three years to providers to help cover the costs of retaining this data. Canada has a data preservation scheme, implemented to enable it to accede to the Budapest Convention.

***International cooperation: Jurisdiction, mutual assistance, and 24/7 point of contact***

29. New Zealand's extradition framework appears to be sufficient for compliance with the Convention. There may need to be legislative changes to enable extra-territorial application of New Zealand jurisdiction, for example where a New Zealander commits an offence outside of the jurisdiction of any state.
30. The Mutual Assistance in Criminal Matters Act 1992 would need to be amended to allow other parties to the Convention to request preservation of data, interception of content data, collection of traffic data, and assistance with access to data in New Zealand where this might assist international investigations. Such amendments were recommended in the 2014 Law Commission report on the Mutual Assistance in Criminal Matters Act 1992, "subject to stringent conditions". Requests from other parties to the Convention would be subject to the existing safeguards in the Mutual Assistance in Criminal Matters Act 1992.
31. On an operational level, we need to consider how to give effect to the requirement for a designated point of contact available on a 24/7 basis, so that other parties to the Convention can get immediate assistance (e.g. evidence gathering and investigation assistance). NZ Police already has a 24/7 operational capacity and might be the most appropriate point of contact.

## **Next Steps**

---

32. The National Cyber Policy Office and Ministry of Justice, working closely with NZ Police, Department of Internal Affairs and other agencies, are leading work to assess in more detail the above requirements.
33. More detailed advice will be provided to relevant Ministers to enable them to decide on New Zealand's approach to the Budapest Convention and the measures required to bring New Zealand's laws and investigative processes into line with it.

## Recommendations

---

34. It is recommended that you:

1. **note** the contents of this aide-memoire.
2. **forward** this aide-memoire to the Minister of Justice.
3. **agree** to engage with the Minister of Justice on the measures required to bring New Zealand's laws and investigative processes into line with the Budapest Convention.
4. **note** that officials from NCPO and Ministry of Justice will provide more detailed advice in due course.



Paul Ash  
Director, National Cyber Policy  
Office, Security and Intelligence

**NOTED**

Hon Clare Curran  
**Minister of Broadcasting,  
Communications and Digital Media**

Date:     /    02    / 2018

Attachment A: List of parties to the Council of Europe Convention on Cybercrime 2001  
(known as the Budapest Convention)

## Attachment A

List of parties to the Council of Europe Convention on Cybercrime 2001 (known as the Budapest Convention)

### Members of Council of Europe

	Signature	Ratification	Entry into Force
Albania	23/11/2001	20/06/2002	01/07/2004
Andorra	23/04/2013	16/11/2016	01/03/2017
Armenia	23/11/2001	12/10/2006	01/02/2007
Austria	23/11/2001	13/06/2012	01/10/2012
Azerbaijan	30/06/2008	15/03/2010	01/07/2010
Belgium	23/11/2001	20/08/2012	01/12/2012
Bosnia and Herzegovina	09/02/2005	19/05/2006	01/09/2006
Bulgaria	23/11/2001	07/04/2005	01/08/2005
Croatia	23/11/2001	17/10/2002	01/07/2004
Cyprus	23/11/2001	19/01/2005	01/05/2005
Czech Republic	09/02/2005	22/08/2013	01/12/2013
Denmark	22/04/2003	21/06/2005	01/10/2005
Estonia	23/11/2001	12/05/2003	01/07/2004
Finland	23/11/2001	24/05/2007	01/09/2007
France	23/11/2001	10/01/2006	01/05/2006
Georgia	01/04/2008	06/06/2012	01/10/2012
Germany	23/11/2001	09/03/2009	01/07/2009
Greece	23/11/2001	25/01/2017	01/05/2017
Hungary	23/11/2001	04/12/2003	01/07/2004
Iceland	30/11/2001	29/01/2007	01/05/2007
Ireland	28/02/2002		
Italy	23/11/2001	05/06/2008	01/10/2008
Latvia	05/05/2004	14/02/2007	01/06/2007
Liechtenstein	17/11/2008	27/01/2016	01/05/2016
Lithuania	23/06/2003	18/03/2004	01/07/2004
Luxembourg	28/01/2003	16/10/2014	01/02/2015
Malta	17/01/2002	12/04/2012	01/08/2012
Monaco	02/05/2013	17/03/2017	01/07/2017
Montenegro	07/04/2005	03/03/2010	01/07/2010
Netherlands	23/11/2001	16/11/2006	01/03/2007
Norway	23/11/2001	30/06/2006	01/10/2006



	Signature	Ratification	Entry into Force
Poland	23/11/2001	20/02/2015	01/06/2015
Portugal	23/11/2001	24/03/2010	01/07/2010
Republic of Moldova	23/11/2001	12/05/2009	01/09/2009
Romania	23/11/2001	12/05/2004	01/09/2004
Russian Federation			
San Marino	17/03/2017		
Serbia	07/04/2005	14/04/2009	01/08/2009
Slovak Republic	04/02/2005	08/01/2008	01/05/2008
Slovenia	24/07/2002	08/09/2004	01/01/2005
Spain	23/11/2001	03/06/2010	01/10/2010
Sweden	23/11/2001		
Switzerland	23/11/2001	21/09/2011	01/01/2012
The former Yugoslav Republic of Macedonia	23/11/2001	15/09/2004	01/01/2005
Turkey	10/11/2010	29/09/2014	01/01/2015
Ukraine	23/11/2001	10/03/2006	01/07/2006
United Kingdom	23/11/2001	25/05/2011	01/09/2011

#### Non-members of Council of Europe

	Signature	Ratification	Entry into Force
Argentina			
Australia		30/11/2012 a	01/03/2013
Cabo Verde			
Canada	23/11/2001	08/07/2015	01/11/2015
Chile		20/04/2017 a	01/08/2017
Colombia			
Costa Rica		22/09/2017 a	01/01/2018
Dominican Republic		07/02/2013 a	01/06/2013
Ghana			
Israel		09/05/2016 a	01/09/2016
Japan	23/11/2001	03/07/2012	01/11/2012
Mauritius		15/11/2013 a	01/03/2014
Mexico			
Morocco			



	Signature	Ratification	Entry into Force
Nigeria			
Panama		05/03/2014 a	01/07/2014
Paraguay			
Peru			
Philippines			
Senegal		16/12/2016 a	01/04/2017
South Africa	23/11/2001		
Sri Lanka		29/05/2015 a	01/09/2015
Tonga		09/05/2017 a	01/09/2017
Tunisia			
United States of America	23/11/2001	29/09/2006	01/01/2007

Total number of signatures not followed by ratifications 4

Total number of ratifications/accessions 56

~~RESTRICTED~~

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



## BRIEFING: Budapest Convention accession – opportunities & analysis

<b>To:</b>	<b>Hon Andrew Little</b> Minister of Justice <b>Hon Kris Faafoi</b> Minister for Broadcasting, Communications and Digital Media
<b>Copy to:</b>	<b>Rt Hon Winston Peters</b> Minister of Foreign Affairs <b>Hon David Parker</b> Attorney-General <b>Hon Stuart Nash</b> Minister of Police <b>Hon Tracey Martin</b> Minister of Internal Affairs <b>Hon Kris Faafoi</b> Minister of Commerce and Consumer Affairs

<b>Date:</b>	9 October 2018	<b>Tracking number:</b>	DPMC-2017/18-1377
<b>Security classification:</b>	RESTRICTED	<b>Priority:</b>	Routine
<b>Action sought:</b>	For decision		
<b>Deadline:</b>	Routine		

Contact for telephone discussion (if required)				
Name	Position	Telephone		1st contact
Paul Ash	Acting Director, National Security Policy Directorate, DPMC	9(2)(a)	9(2)(a)	✓
6(a)	Policy Advisor, National Security Policy Directorate, DPMC	9(2)(a)	9(2)(a)	
Stuart McGilvray	Policy Manager, Criminal Law, Ministry of Justice	9(2)(a)		

~~RESTRICTED~~

~~RESTRICTED~~

**Agencies consulted**

New Zealand Police; Ministry of Foreign Affairs and Trade; Ministry of Business, Innovation, and Employment; Department of Internal Affairs; Crown Law; New Zealand Customs; Government Communications Security Bureau

**Minister's office to complete:**

☐ Approved

☐ Declined

☐ Noted

☐ Needs change

☐ Seen

☐ Overtaken by Events

☐ See Minister's Notes

☐ Withdrawn

**Comments**

Released under the Official Information Act 1982

~~RESTRICTED~~



## BRIEFING: Budapest Convention accession – opportunities & analysis

### Purpose

To provide you with an overview of the Council of Europe Convention on Cybercrime (the Budapest Convention), the benefits of accession, and to describe the process by which New Zealand can accede to the Convention.

### Recommendations

The Ministry of Justice and Department of the Prime Minister and Cabinet recommend that you:

- |   |   |                       |
|---|---|-----------------------|
| 1 | <b>Agree</b> that the Minister of Justice and the Minister for Broadcasting, Communications and Digital Media will seek Cabinet agreement to accede to the Council of Europe Convention on Cybercrime (Budapest Convention);        | <b>Agree/Disagree</b> |
| 2 | <b>Note</b> that legislative amendments will be required in order to accede to the Budapest Convention;   |                       |
| 3 | <b>Agree</b> that the legislative amendments will be made via an omnibus Bill made for the purpose of acceding to the Budapest Convention;  | <b>Agree/Disagree</b> |
| 4 | <b>Note</b> that if this work progresses, other items in the Ministry of Justice work programme may need to be re-prioritised.  | <b>Agree/Disagree</b> |
| 5 | <b>Agree</b> for officials from the Ministry of Justice and Department of the Prime Minister and Cabinet to prepare a Cabinet paper and National Interest Analysis recommending that New Zealand accede to the Budapest Convention; | <b>Agree/Disagree</b> |
| 6 | <b>Agree</b> that officials will undertake a consultation process with telecommunications companies on the costs of a data preservation scheme.   | <b>Agree/Disagree</b> |
| 7 | <b>Forward</b> this briefing to Rt Hon Winston Peters, Minister of Foreign Affairs;   | <b>Agree/Disagree</b> |
| 8 | <b>Forward</b> this briefing to Hon David Parker, Attorney-General;   | <b>Agree/Disagree</b> |



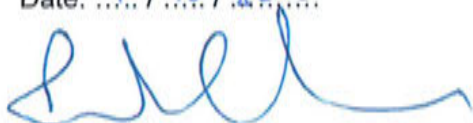
RESTRICTED

- |    |   |                       |
|----|---|-----------------------|
| 9  | <b>Forward</b> this briefing to Hon Stuart Nash, Minister of Police;                        | <b>Agree/Disagree</b> |
| 10 | <b>Forward</b> this briefing to Hon Tracey Martin, Minister of Internal Affairs;            | <b>Agree/Disagree</b> |
| 11 | <b>Forward</b> this briefing to Hon Kris Faafoi, Minister of Commerce and Consumer Affairs. | <b>Agree/Disagree</b> |



Stuart McGilvray  
Policy Manager, Criminal Law  
**Ministry of Justice**

Date: 9 / 10 / 2018



Paul Ash  
Acting Director, National Security Policy  
Directorate  
**Department of the Prime Minister and  
Cabinet**

Date: 9 / 10 / 2018

Hon Andrew Little  
**Minister of Justice**

Date: .... / .... / .....

Hon Kris Faafoi  
**Minister for Broadcasting, Communications  
and Digital Media**

Date: .... / .... / .....

## Introduction

1. The Council of Europe Convention on Cybercrime (more commonly known as the "Budapest Convention") was adopted by the Council of Europe in 2001 and is the first international treaty seeking to address Internet and computer crime. The Convention does so by harmonising national laws, improving investigative techniques, and increasing international law enforcement cooperation. The Budapest Convention provides an international best practice standard and benchmark in relation to cybercrime laws.
2. Despite its Council of Europe origins, the Convention is open to accession by all states by invitation. The Budapest Convention has 59 members as of September 2018. Parties to the Budapest Convention include all of New Zealand's Five Eyes partners<sup>1</sup>, and countries such as Tonga, Sri Lanka, and Nigeria. So far in 2018, the Philippines, Morocco, and Samoa have all acceded.
3. The Convention requires parties to adopt a number of measures in order to improve international responses to cybercrime. International cooperation is necessary to effectively address cybercrime because the perpetrators are often based overseas, presenting real investigative and prosecutorial challenges for law enforcement agencies.

## The cybercrime context

4. Cybercrime is defined in New Zealand's *National Plan to Address Cybercrime, 2015*:
  - a. "For the purposes of this Plan, the definition of cybercrime has two elements.
    - i. A criminal act that can only be committed through the use of ICT or the Internet and where the computer or network is the target of the offence. This is regardless of what the criminal goal is – whether political or financial gain, espionage or any other reason. Examples of cybercrime include producing malicious software, network intrusions, denial of service attacks and phishing.
    - ii. Cyber-enabled crime is any criminal act that could be committed without ICT or the Internet, but is assisted, facilitated or escalated in scale by the use of technology. This includes a vast amount of serious and organised crime, such as cyber-enabled fraud or the distribution of child exploitation material."
5. The Budapest Convention addresses both 'pure' cybercrime and cyber-enabled crime. Throughout this briefing, use of the word 'cybercrime' will refer to both types.
6. Cybercrime frequently occurs across borders, and attacks are often launched through machines in third countries, exploiting the uneven landscape of cyber-related laws across different jurisdictions. Cybercrime investigations often rely on information and evidence held in other jurisdictions. Mutual assistance legislation, treaties and arrangements exist but these can be slow and complex to navigate, and are not suited to high volume, low value crimes such as fraudulent scamming. While the Budapest Convention does not fix this problem completely, accession can facilitate access to

<sup>1</sup> The United Kingdom, Australia, Canada and the United States of America.

information held by other parties to the Convention, and assist with working collaboratively across borders on such problems.

### **Measures required by the Budapest Convention**

7. In order to standardise national laws relating to cybercrime offences, parties must ensure the following offences are incorporated in their domestic laws:
  - a. offences against the confidentiality, integrity and availability of computer data and systems (e.g. illegal access to computer systems, illegal interception of computer data, interference with computer data, interference with the functioning of computer systems, and misuse of computer devices);
  - b. computer-related offences such as fraud or forgery;
  - c. content-related offences such as the distribution of child pornography through computer systems; and
  - d. offences related to infringements of copyright and theft of intellectual property.
8. The Convention also requires parties to adopt certain powers and procedures for investigating cybercrime offences, consistent with domestic and international human rights obligations and other safeguards. The powers and procedures include:
  - a. measures to order the expeditious preservation of computer data and computer traffic data for up to 90 days;
  - b. measures to order the production of specified computer data and subscriber information (Production Orders);
  - c. measures to enable search and seizure of stored computer data;
  - d. measures to collect computer traffic data<sup>2</sup> associated with specified communications in real time; and
  - e. in relation to serious offences, measures to collect computer content data in real time.
9. The Convention further sets out a number of principles and procedures related to international cooperation amongst the parties on investigating cybercrime. This includes:
  - a. deeming the cybercrime offences listed above as extraditable offences;
  - b. procedures relating to mutual assistance and sharing of information in the investigation of cybercrime offences;

<sup>2</sup> Commonly known as 'metadata', which is data about data. New Zealand's Telecommunications (Interception Capability & Security) Act 2013 uses the terminology 'call associated data', which is a certain subset of metadata (in section 3). In the cybercrime context, this can include call duration, phone numbers, IP addresses, and so forth. This can, in certain circumstances, be just as important as the actual content data the metadata is 'about'.

- c. provisions for mutual assistance between parties on expeditious preservation of computer data and computer traffic data, and access to computer data and computer traffic data; and
- d. the establishment of a 24 hour/7 day a week designated point of contact to ensure the provision of assistance between parties for the investigation of cybercrime.

## Benefits and opportunities of accession to the Convention

10. Accession to the Convention would have significant reputational value for New Zealand. It would signal that we take cybercrime seriously and demonstrate our support for the best practice standards established by the Convention. <sup>6(a)</sup>

11. <sup>6(a), 6(b)</sup>

12. Accession to the Convention would also give New Zealand better access to international dialogue on cybercrime, from the point at which we formally express interest in acceding. Much of the international dialogue on cybercrime-related issues happens within the context of the Budapest Convention. If New Zealand were a party to the Convention, we would be able to obtain additional international advantages:

- a. Parties to the Convention are automatically members of the Cybercrime Convention Committee (T-CY), which is currently the most relevant intergovernmental body dealing with cybercrime.
- b. Within the context of the T-CY, there are negotiations aimed at developing the law on international cybercrime issues. Currently there are ongoing negotiations on an Additional Protocol to the Convention, on access to evidence in "the cloud"<sup>3</sup>.
- c. Capacity building on cybercrime (for example, legislation, judicial training, improving interagency co-operation) occurs among state parties to the Convention.

13. Accession to the Budapest Convention has also been recognised domestically as desirable:

- a. It was included in *New Zealand's Cyber Security Strategy 2011*, and in the Action Plan of *New Zealand's Cyber Security Strategy 2015*. With a refresh of New Zealand's cyber security strategy currently underway, officials from all relevant

<sup>3</sup> From: <https://www.recode.net/2015/4/30/11562024/too-embarrassed-to-ask-what-is-the-cloud-and-how-does-it-work>: "The cloud" refers to software and services that run on the Internet, instead of locally on a computer. Most cloud services can be accessed through a Web browser like Firefox or Google Chrome, and some companies offer dedicated mobile apps. Some examples of cloud services include Google Drive, Apple iCloud, Netflix, Yahoo Mail, Dropbox and Microsoft OneDrive." There are issues with access to this evidence, including identifying where the data is held, and serving domestic orders on international companies.




agencies are agreed that accession to the Budapest Convention will provide a range of benefits and opportunities for New Zealand.

- b. The Law Commission and the Ministry of Justice in their 2016 joint review of the Search and Surveillance Act <sup>4</sup> recommended that "[t]he Government should consider whether New Zealand should accede to the Council of Europe Convention on Cybercrime ETS 185 (Budapest Convention)". The Law Commission issues paper on Extradition and Mutual Assistance also noted that there are very good reasons for New Zealand to sign and ratify the Budapest Convention.<sup>5</sup> These include its multilateral nature, number of existing parties and proven practicality.

### Benefits for New Zealand's law enforcement agencies

14. Critically, being a party to the Budapest Convention would give operational agencies better access to data flows on cybercrime – both investigative data that can be used as evidence in criminal cases, and for interagency information sharing that can be used to prevent cybercrime and reduce victimisation. These information flows are critical, given the transnational nature of computer crime. Accession would enable New Zealand to more easily obtain assistance, and 'best practice' information from other parties to the Convention, especially countries that we do not currently have other arrangements with: for example, individual European countries, Europol (the law enforcement agency of the European Union), and other parties to the Convention such as South Africa, Mexico, and Japan.
15. In New Zealand, the main law enforcement agencies involved in the investigation of cybercrime are units within the New Zealand Police (High Tech Crime Unit), and the Department of Internal Affairs (Electronic Messaging Compliance Unit and Digital Child Exploitation Team). Accession to the Convention would enhance both agencies' ability to effectively do their jobs.
16. Police and DIA have provided some specific examples of where investigations could have been more effective, had New Zealand been a state party to the Budapest Convention accession, as follows:

6(a), 6(b)




<sup>4</sup> Law Commission *Review of the Search and Surveillance Act 2012*

<http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC-R141-Review-of-the-Search-and-Surveillance-Act-2012-final.pdf>


<sup>5</sup> Law Commission *Extradition and Mutual Assistance in Criminal Matters*

<https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20IP37.pdf>

6(a), 6(b)




6(a), 6(b)




17. A range of law enforcement functions in New Zealand could also benefit from the increased access to data as a result of accession to the Convention. This is because cybercrime also encompasses frauds, scams, and thefts, most of which is now crime committed online. Additionally, a great deal of evidence for all types of crime (for example, drug crime and other types of trans-national organised crime) can be stored on computer systems.

18. Accession to the Convention is also used as a benchmark to assess the adequacy of a country's laws on computer crime – including its civil rights protections in investigations involving computers.


19. 6(a), 9(2)(f)(iv)



20. 6(a), 9(2)(f)(iv)



6(a), 6(b)



6(a), 6(b)

## Legislative requirements for accession

21. If a decision is made to accede to the Budapest Convention, New Zealand will need to make changes to the following legislation in order to implement the Convention:

- a. the Search and Surveillance Act 2012;
- b. the Crimes Act 1961; and
- c. the Mutual Assistance in Criminal Matters Act 1992.

22. The most significant of the necessary legislative changes are detailed under the following headings. There is a series of smaller amendments that will need to be made to these Acts, detailed in Attachment A.

23. A decision will also need to be made about the most appropriate legislative vehicle to make these changes. The two options are:

a. 9(2)(f)(iv)

b.

24. The Ministry of Justice already has a significant work programme, including legislative work, which these reforms will have to be added to. It may be possible for DPMC to work in collaboration with Justice to share the work, but other work on the Justice work programme may have to be re-prioritised if Ministers wish to progress this work. It should be possible to have an omnibus Bill to give effect to the necessary changes introduced to the House at the end of 2019.

9(2)(f)(iv)

<sup>8</sup> "Extradition and Mutual Assistance in Criminal Matters" <http://lawcom.govt.nz/our-projects/extradition-and-mutual-assistance-criminal-matters?id=1292> and Review of the Search and Surveillance Act 2012 <http://lawcom.govt.nz/our-projects/search-surveillance-act-2012?id=1498>.



## Data preservation orders

25. The most significant legislative instrument that we will need to introduce in order to accede is a 'data preservation order'. This mechanism could be inserted into the Search and Surveillance Act 2012.
26. If these orders were introduced, entities that hold specific information relevant to a specific criminal investigation could be required to temporarily preserve that information, while a search warrant or production order is sought. Preservation orders would not allow law enforcement to view or take possession of data; only to 'freeze' it and ensure the information is not deleted. Convention countries must also be able to access each other's preservation order schemes. This means that data preservation orders would have real value in international investigations – both to and from New Zealand.
27. These orders are beneficial because computer data can be routinely deleted within hours or days of its creation. This creates problems for law enforcement, as frequently it takes several days to obtain a production order. By the time a production order comes into force, the relevant information may no longer be stored. Such information is also increasingly critical to investigate a wider range of offences beyond pure cybercrime, such as organised crime. The Crown Law Office has indicated that it can, in some cases, take six to 18 months for the formal mutual assistance process to be completed.
28. The Law Commission report noted that New Zealand telecommunications companies (frequently the holders of data that would need to be preserved) currently preserve this data on an informal basis following a request from law enforcement. <sup>6(b)</sup>
29. There is still merit in formalising this process, however, as it will allow for greater transparency and certainty. The private sector sought and received similar certainty in respect of compulsion relating to the production of business records, as the Intelligence and Security Act 2017 was being developed.
30. Additionally, the 'informal preservation' status quo is changing. The New Zealand telecommunications industry has recently set strong signals of their intention to move to routine mass deletion of both content data and process/meta data when no longer required for business purposes (30 days post billing or less).
31. It is important to note that data preservation is different from data retention. Data preservation orders are issued to 'freeze' a discrete amount of data for a specific investigation. In contrast, data retention orders require entities to store all or most of their data, in bulk, for a certain time period. The Budapest Convention does not require state parties to have data retention mechanisms. However, New Zealand's operational agencies rely on stored data to solve a range of crime. <sup>9(2)(g)(i)</sup>

### Consultation on data preservation

32. Introducing data preservation orders into the Search and Surveillance Act will require consideration of a range of issues, including:

- a. the time periods for preservation;
- b. the level of 'seriousness' of offences that preservation orders can apply to;
- c. whether preservation is prospective/'forward looking' (i.e. there is an ongoing obligation to capture and preserve data for the duration of the order);

These issues will be considered in more depth if a decision is made to accede.

33. There will also be cost implications for telecommunications companies in introducing a data preservation scheme; in both obtaining the necessary equipment and for ongoing compliance. These costs are difficult to quantify, as they depend on many factors - including those in the previous paragraph, and whether (for example) industry can extract and provide stored data using the same technology and format currently used by law enforcement.<sup>9(2)(ba)(i)</sup>

34. Officials therefore propose to undergo an external engagement process with telecommunications companies before seeking Cabinet agreement to accede to better quantify this cost - and, subsequently, where it might fall. This will enable the Cabinet paper and National Interest Analysis to include better information on the costs of accession to the Convention.

### Mutual assistance for interception warrants

35. The Mutual Assistance in Criminal Matters Act 1992 would need to be amended to allow other parties to the Convention to request preservation of data, interception of content data, collection of traffic data, and assistance with access to data in New Zealand where this might assist international investigations, as required by Articles 33 and 34 of the Convention.

36. Articles 33 and 34 are the subject of some criticism from nations<sup>6(a)</sup> who claim that they infringe upon state sovereignty. However, requests from other parties to the Convention would be subject to the existing safeguards in the Mutual Assistance in Criminal Matters Act 1992, and to the protections in the Budapest Convention stating that this mutual assistance is to be "governed by the conditions and procedures provided for under domestic law."

### Third-party confidentiality orders

37. For two of the powers required by the Convention - real-time collection of traffic data and interception of content data - the Convention requires parties to adopt "legislative and other measures as may be necessary" to keep the execution of those powers confidential. This would cover, for example, legal measures for confidentiality from telecommunications provider<sup>9(2)(g)(i)</sup>, where the Police need to obtain<sup>9(2)(g)(i)</sup> assistance

in intercepting communications over a phone line. New Zealand currently has no formal measures of this kind - only informal 'contractual-style' confidentiality arrangements covering third parties that receive a surveillance warrant.

38. Officials therefore recommend introducing a power to issue third-party confidentiality orders in the Search and Surveillance Act 2012, i.e. stopping third parties aware of a law enforcement order (like a telecommunications company) from informing the subject of the order of the fact it exists. This would also have to be made available in a Mutual Assistance in Criminal Matters context.

*Confidentiality issues where evidence is sent overseas*

39. Additionally, there is a related issue in the mutual assistance context. In the *Dotcom* Supreme Court decision,<sup>9</sup> the Court held that the Attorney-General should advise any affected party in advance of their intention to send material obtained by a search warrant or a production order offshore. In doing so, the affected party would have the opportunity for a legal challenge.

40. However, this means that law enforcement is no longer able to rely on the delayed notice provisions of the Search and Surveillance Act<sup>10</sup> (which would otherwise be applicable to Mutual Assistance in Criminal Matters Act search warrants), therefore preventing these search warrants from remaining confidential.

41. <sup>9</sup>(2)(h)

The Convention does not specifically require this type of confidentiality, but it may be that to give efficacy to mutual assistance where a search is confidential (in the spirit of the Convention) that the Search and Surveillance Act delayed notice provisions should be amended. These amendments would confirm that the delayed notice provisions apply in the Mutual Assistance in Criminal Matters Act context, notwithstanding the Supreme Court's comments in the *Dotcom* decision.

## Risks, perceptions, and alternatives

42. The legislative requirements for accession, detailed below and in Attachment A, carry some public perception risks; officials consider that these will be far outweighed by the benefits already discussed. These include:

- a. A perception that New Zealand is looking to implement a data retention scheme. As noted above, data preservation is different from data retention. Data retention has a different set of requirements to data preservation: the Convention requires the latter. Data retention has proven more controversial in some jurisdictions. This risk is able to be mitigated with clear talking points and messaging on the issue.

<sup>9</sup> *Dotcom v Attorney-General* [2014] NZSC 199; [2015] 1 NZLR 746 at [201]

<sup>10</sup> Search and Surveillance Act 2012, ss 134-135



- b. The response of Internet community to New Zealand's accession. This is likely to be positive: for example, InternetNZ has previously encouraged accession.<sup>11</sup> However, as some of the legislative changes will enable easier law enforcement access to data, there may be some controversy. It is important to note that the Convention itself discusses the importance of human rights, and that both New Zealand law and the Convention both contain sufficient appropriate safeguards.
43. In terms of alternatives to the Convention on international co-operation on cybercrime, there are very few. The Convention is currently a best practise standard and a benchmark for international co-operation on cybercrime. Much discussion on computer crime and its investigation, in the international context, occurs within the context of the Convention.
44. As detailed earlier, data preservation will also carry cost impacts. These are yet to be determined. The parameters of the scheme will determine how large the cost will be, and these will become clearer during the proposed external engagement process with telecommunications companies.

## Process for accession

### Council of Europe process

45. As New Zealand is not a Council of Europe member, we must be invited by them to accede to the Convention. The Council have advised that it is customary for states to formally express interest in accession to the Council of Europe through a letter to their Secretariat from the Minister of Foreign Affairs. The Council of Europe would then consider whether to issue an invitation allowing New Zealand to accede to the Convention.<sup>6(b)</sup>

46. Once this invitation is received, New Zealand will then enter into an informal status as an invited party with the Council of Europe, known as the 'on-ramp.' This provides New Zealand with some access to the benefits of the Convention while amending our legislation and processes as necessary to fully comply with the Convention. While on the 'on-ramp', New Zealand would have opportunities to make law enforcement connections and would be able to attend the T-CY as an observer. Observer status would allow New Zealand to participate in the current development of rules around international cooperation and access to evidence in the cloud, which are being negotiated as part of the Additional Protocol to the Convention. Formal accession must then take place within five years.

### New Zealand process

47. To take into account the need to seek an invitation to accede from the Council of Europe, we propose the following process:

<sup>11</sup> <https://internetnz.nz/blog/links-thinks-refreshing-cybersecurity-strategy>

- a. Cabinet approval is sought for New Zealand to request an invitation to accede from the Council of Europe and to have the Convention and an accompanying National Interest Analysis presented to the House of Representatives for parliamentary treaty examination. It would be a joint Cabinet paper from the Minister of Justice and the Minister of Broadcasting, Communications and Digital Media. That Cabinet paper will also seek authorisation to issue drafting instructions to the Parliamentary Counsel Office regarding implementing legislation.

The Convention and the National Interest Analysis will then be presented to the House of Representatives for parliamentary treaty examination. Once this process has been completed, the Minister of Foreign Affairs will then send the letter expressing interest in accession to the Council of Europe, beginning the process outlined above.

## Next Steps

48. If you agree, the next steps in this process are:

- a. For officials to begin consultation with the telecommunications industry, regarding the costs of accession to the Convention.
- b. Development of a joint Cabinet paper from the Minister of Justice and the Minister of Broadcasting, Communications and Digital Media and an accompanying National Interest Analysis.

## Attachment A – Minor legislative amendments required for accession to the Budapest Convention

This attachment discusses less significant legislative amendments that will need to be made to legislation, in order to accede to the Budapest Convention (see the main body of the briefing for more significant amendments). The necessary amendments to legislation are organised by the article of the Convention that they would enable accession to.

### Article 5

1. This Article requires "the serious hindering without right of the functioning of a computer system" to be an offence. Our relevant offence is s 250 of the Crimes Act. It discusses causing a computer system to "fail" or "deny service to any authorised users", but these do not cover every situation where a computer system's function might be hindered.

9(2)(f)(iv)

### Article 6

2. This Article prohibits certain acts regarding the tools of computer crime – software, information, and devices. Our relevant parts of the Crimes Act are section 251 (software & information) and sections 228A-C (devices). Both need to be amended to be compliant.

9(2)(f)(iv)

9(2)(f)(iv), 9(2)(g)(i)



9(2)(f)(iv)

6. **Purpose of the Tool:** Sub-article 1 requires the tools to be able to be used "for the purposes of committing any of the offences established in Articles 2 through 5." Section 251 relates only to software that enables a person to access a computer system without authorisation.

9(2)(f)(iv)

## Article 22

8. This requires that parties establish jurisdiction over Convention offences "[W]hen the offence is committed [...] by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State" (art 22(1)(d)).

9(2)(f)(iv), 9(2)(g)(i)



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

# Aide-Memoire

## RELEASE OF DATA PRESERVATION CONSULTATION PAPER

To	Minister of Justice (Hon Andrew Little) Minister of Broadcasting, Communications and Digital Media (Hon Kris Faafoi)		
From	Paul Ash, Acting Director, National Security Policy Directorate, DPMC	Report No	1819NSP/044
		Date	22/11/2018

### Purpose

- To notify you that the attached Data Preservation Consultation Paper will be dispatched to telecommunications companies and government agencies, and to seek your agreement to this.

### Background

- In an earlier briefing dated 9 October, 'Budapest Convention accession – opportunities and analysis', you agreed "that officials will undertake a consultation process with telecommunications companies on the costs of a data preservation scheme".
- Officials from MBIE, DPMC, and the Ministry of Justice have subsequently prepared the attached Consultation Paper in consultation with Police, DIA, and Crown Law. It is designed to discuss the initial costs of the data preservation scheme required in order to accede to the Council of Europe Convention on Cybercrime (Budapest Convention). It will be dispatched, once you agree, to telecommunications companies and government stakeholders.
- The responses received from this Consultation Paper will be inserted into the Cabinet paper seeking agreement for New Zealand to formally request an invitation to accede to the Budapest Convention, in order to describe the financial implications of doing so.

Attachments:	
Attachment A	Data Preservation Consultation Paper

## Recommendations

1. It is recommended that you **note** the contents of this aide-memoire.
2. It is recommended you **agree** to the release of the attached consultation paper to telecommunications companies and government stakeholders for feedback.

Agree / Disagree

NOTED

Hon Andrew Little  
**Minister of Justice**

Date:     /     / 2018

  
Paul Ash  
**Acting Director, National  
Security Policy Directorate**

Department of the Prime  
Minister and Cabinet

Date: 23 / 11 / 2018

Hon Kris Faafoi  
**Minister of Broadcasting, Communications and  
Digital Media**

Date:     /     / 2018





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

# Aide-Memoire

## FOLLOW-UP: RELEASE OF DATA PRESERVATION CONSULTATION PAPER

<b>To</b>	Minister of Justice (Hon Andrew Little) Minister of Broadcasting, Communications and Digital Media (Hon Kris Faafoi)		
<b>From</b>	Paul Ash, Acting Director, National Security Policy Directorate, DPMC	<b>Report No</b>	1819NSP/060
		<b>Date</b>	7/12/2018

### Purpose

- To provide you an updated copy of the attached Data Preservation Consultation Paper (previously dispatched to you on the 22 November 2018), after the incorporation of feedback from Minister Faafoi.
- This will be dispatched to telecommunications companies and government agencies, once you agree. Agencies are aiming to dispatch ahead of the Christmas break.

### Background

1. In an earlier briefing dated 9 October, 'Budapest Convention accession – opportunities and analysis', you agreed "that officials will undertake a consultation process with telecommunications companies on the costs of a data preservation scheme".
2. Officials from MBIE, DPMC, and the Ministry of Justice subsequently prepared a consultation paper in consultation with Police, DIA, and Crown Law. It is designed to discuss the initial costs of the data preservation scheme required in order to accede to the Council of Europe Convention on Cybercrime (Budapest Convention).
3. The responses received from this Consultation Paper will inform the financial implications section of a Cabinet paper seeking agreement for New Zealand to formally request an invitation to accede to the Budapest Convention.
4. Minister Faafoi has returned the paper with feedback to be incorporated, which has been actioned:

- An extended timeline for consultation (due date now Monday 25<sup>th</sup> February 2019) on page 4;
  - Drawing more attention to the opinion of the Law Commission on data preservation on page 6;
  - Adding a flow diagram to describe the practical application of a data preservation order on page 7;
  - Asking respondents to indicate any sensitive commercial information in their responses.
5. We also intend to consult with overseas law enforcement partners on their experiences with their data preservation schemes. This will give us more information on key points, including the number of data preservation orders we may be able to expect from other countries.
6. This will be dispatched to telecommunications companies and government agencies, once you agree. DPMC and MBIE are aiming to dispatch ahead of the Christmas break.

<b>Attachments:</b>	
<b>Attachment A</b>	Data Preservation Consultation Paper (updated).

## Recommendations

---

1. It is recommended that you:

- a. **note** the contents of this aide-memoire;
- b. **agree** to the release of the attached consultation paper to telecommunications companies and government stakeholders for feedback.

Yes / No

Paul Ash  
**Acting Director, National Security  
 Policy Directorate**  
 Department of the Prime Minister and  
 Cabinet

Date:     /     / 2018

### NOTED

Hon Andrew Little  
**Minister of Justice**

Date:     /     / 2018

Hon Kris Faafoi  
**Minister of Broadcasting, Communications  
 and Digital Media**

Date:     /     / 2018





---

# **DATA PRESERVATION CONSULTATION PAPER**

**Towards accession to the Council of Europe Convention on  
Cybercrime**

---

March 2019

Released under the Official Information Act 1982

## Contents

Purpose .....	3
Request for submissions .....	4
Important notice .....	4
Background .....	5
The Budapest Convention.....	5
Acceding to the Budapest Convention: proactively tackling cybercrime .....	5
Data preservation orders .....	6
Benefits of data preservation orders .....	6
Current state .....	6
In practice .....	7
PART I: PARAMETERS OF DATA PRESERVATION .....	8
Duration of preservation .....	8
Foreign preservation orders .....	8
Forward-looking preservation orders .....	9
Types of data to preserve .....	10
Penalties for non-compliance with a preservation order .....	11
PART II: COSTS AND FUNDING OF A DATA PRESERVATION REGIME .....	12
Categories of costs .....	12
Quantifying costs .....	12
Number of orders .....	12
Allocation of costs .....	13
Full list of questions .....	14

## Purpose

DPMC and MBIE are seeking feedback from telecommunications operators on the potential costs and practicalities of introducing a data preservation scheme in New Zealand.

A data preservation scheme would require entities that hold information relevant to a specific criminal investigation to temporarily preserve that information, while a production order is sought. It is one of a number of potential legislative changes required to allow the New Zealand Government to accede to the Council of Europe Convention on Cybercrime, otherwise known as the Budapest Convention ("the Convention"). Accession to the Convention would help to improve Government's ability to proactively prevent, investigate, deter and respond to cybercrime.

Your feedback will be used to inform analysis of the costs and benefits of introducing a data preservation scheme. This is part of a policy process to inform a decision on accession to the Convention.

If the Government decides to accede to the Convention and make changes to legislation, there will also be a further opportunity to make a submission on data preservation (and a broader range of issues) to a Parliamentary Select Committee. Select Committees seek submissions from the public and must consider any proposed changes before legislation is passed.



## Request for submissions

You are invited to make a written submission on the issues raised in this paper. The closing date for submissions is **5pm, Monday 1 April 2019**.

Specific questions are listed at the end of relevant sections, and the full set of questions is listed at the end of this document. If you feel particular questions are not relevant to you or you do not have any particular opinion on a question, then please only answer the questions that are relevant to you.

We are seeking specific examples, evidence and data to inform our final policy decisions. Your responses will be treated as commercial in confidence: please indicate if specific information is commercially sensitive. There are no plans to publish this paper or submissions on it, though submissions will be subject to the Official Information Act, subject to redaction of sensitive commercial information.

Additionally, as this consultation paper is intended to inform a costs analysis, it would be helpful if submissions could indicate whether the different policy options will have an impact on the costs of preservation, and the extent of this cost impact, including comparisons where possible (e.g. X will have the greatest impact on costs of all of the options discussed in this paper.)

You can make your submission by emailing it as a Microsoft Word document or PDF to [communicationspolicy@mbie.govt.nz](mailto:communicationspolicy@mbie.govt.nz).

## Important notice

*While your responses to this paper will be treated as commercial in confidence, submissions will be subject to the provisions of the Official Information Act 1982.*

*This consultation paper is not Government policy. The opinions contained in this document are those of the Ministry of Business, Innovation and Employment and the Department of the Prime Minister and Cabinet.*

*The contents of this consultation paper must not be construed as legal advice. The Ministry and the Department do not accept any responsibility or liability whatsoever for any action taken as a result of reading, or reliance placed on the Ministry and the Department because of having read, any part, or all, of the information in this consultation paper or for any error, inadequacy, deficiency, flaw in or omission from the consultation paper.*

## Background

### The Budapest Convention

The Budapest Convention was adopted by the Council of Europe in 2001. It is the first international treaty seeking to address internet and computer crime. It does so by harmonising national laws, improving investigative techniques, and increasing international law enforcement cooperation. The Convention provides an international best practice standard and benchmark in relation to cybercrime laws.

Accession to the Convention forms a part of improving New Zealand's posture in relation to cyber security and cybercrime, and has long been a part of the Government's work programme on cybercrime, including in New Zealand's Cyber Security Strategy 2011, and in the Action Plan of New Zealand's Cyber Security Strategy 2015. Other actions achieved to date under the 2015 Strategy include the establishment of CERT NZ to respond to cyber security threats in New Zealand, the rollout of the CORTEX initiative by the Government Communications Security Bureau, and the establishment of a Level 6 Diploma in Cyber Security.

### Acceding to the Budapest Convention: proactively tackling cybercrime

Internet connectivity brings New Zealand to the world, underpins our prosperity, and helps to negate the downsides of distance. However, these new opportunities sit alongside an evolving cyber security risk. Cyber enabled threats, including cybercrime, continue to grow in number, scope, and scale.

Cybercrime frequently occurs across borders, and attacks are often launched using third countries, exploiting the uneven landscape of cyber-related laws across different jurisdictions. Cybercrime investigations often rely on information and evidence held in other countries and mutual assistance legislative arrangements can be slow and complex to navigate, undermining effective law enforcement outcomes.

Given these challenges, the Convention will help achieve better responses to cybercrime in New Zealand by:

- Making sure our criminal law is able to more effectively address cybercrime.
- Enabling us to receive information for investigations and prosecutions.
- Ensuring efficient international cooperation for law enforcement purposes.

Government and industry have shared interests in addressing cybercrime. Both benefit from seeing the number of cybercrimes decreasing; from cybercrime being more effectively investigated where it occurs; and from the related cost savings and reputational benefits.

## Data preservation orders

### Benefits of data preservation orders

The Convention requires countries to have a data preservation scheme in place to accede. With a data preservation scheme in place, entities that hold information relevant to a specific criminal investigation could be required to temporarily preserve that information, while a production order is sought.

A 2017 report by the Law Commission and the Ministry of Justice (“the Law Commission report”) recommended that a data preservation regime be “tightly constrained” and “should not extend significantly beyond [the Convention’s] requirements.”<sup>1</sup>

Aside from the benefits of acceding to the Convention, data preservation orders could help New Zealand to proactively tackle cybercrime by:

- Ensuring that communications data is reasonably accessible to law enforcement agencies, while maintaining New Zealand’s long-held commitment to protecting privacy interests.
- Ensuring that New Zealand law is sufficiently harmonised with that of its international partners, so that efficient co-operation is enabled.
- Formalising and making more transparent law enforcement’s existing arrangements for preservation of data in New Zealand.

### Current state

Law enforcement currently gains the information it needs using different types of orders:

- **Search warrants** – law enforcement agencies use these where they need to physically enter and search a person or a location.
- **Production orders** – these are used to require a custodian of documents to deliver them or make them available.
- **Surveillance device warrants** – these are used to undertake surveillance or intercept communications.
- **Examination orders** – these are used to require a person to answer questions in a specific set of circumstances, when they have previously refused to do so.

Preservation orders would be an additional type of order law enforcement agencies can use, usually to be followed by a production order. They could be used where obtaining a production order would be too slow to obtain the data in time (e.g. the data is particularly susceptible to loss or modification; or the production order comes from overseas so a specific legal process is required, which can take a long time).

---

<sup>1</sup> <https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC-R141-Review-of-the-Search-and-Surveillance-Act-2012-final.pdf> at paragraphs 14.140-14.144.

New Zealand Police contributes to the costs of telecommunications companies complying with the different types of orders above, currently funding 5,000 – 6,000 production orders per annum with the three main telecommunications operators.

It is also important to recognise that data preservation is distinct from data retention. A data retention regime would require entities to store all or most of their metadata, in bulk, for a certain time period.

### In practice



Data preservation orders would only be available for computer data that is stored in the normal course of business (both content data and metadata).

A data preservation scheme does not allow law enforcement to view or take possession of data without a warrant or production order. It only requires the holders of the data to ensure it is not deleted.



## PART I: PARAMETERS OF DATA PRESERVATION

Part I outlines some possible parameters of a data preservation regime and asks about their resourcing impacts, limitations, and related challenges.

### Duration of preservation

We are seeking views on the extent to which preserving data for a longer period impacts the costs or difficulties of doing so.

The Convention states that preservation be available for “as long as necessary, up to a maximum of ninety days [...] A Party may provide for such an order to be subsequently renewed.” The Law Commission report recommended that the initial preservation order be effective for no more than 20 days, and that this timeframe should be able to be extended for up to 90 days.<sup>2</sup>

Additionally, we are seeking views on:

- Whether law enforcement agencies should be compelled to serve notice discontinuing a preservation order if the grounds upon which the order was made no longer exist; or the investigation to which it relates to is otherwise discontinued.
- Whether legislation should mandate that preserved data must be destroyed after a preservation order expires. Canadian legislation requires this.<sup>3</sup>

**Question 1:** Would there be any challenges in preserving the data for 20 days? What would these be?

**Question 2:** How would extending the time period for preservation orders impact the difficulty of being able to carry them out?

**Question 3:** Would an extension of the order cause any additional challenges?

**Question 4:** Should legislation specify that preservation orders be discontinued if no longer applicable? Why/why not?

**Question 5:** After a preservation order ends, should data be destroyed when a notice is received? What procedural challenges could this create?

### Foreign preservation orders

Accession to the Convention would require New Zealand to make provision for the preservation of data at the request of foreign jurisdictions who are also signatories to the Convention.<sup>4</sup> It is proposed that New Zealand make provision for foreign preservation orders that would parallel, or nearly

---

<sup>2</sup> Recommendation 53.

<sup>3</sup> Canadian Criminal Code, s 487.0194(2).

<sup>4</sup> At Article 29.

parallel, domestic preservation orders.<sup>5</sup> The only difference that would relate to costs would be the duration of the order.

This is because while the mutual legal assistance regime provides a structured and transparent process for information-sharing, it is recognised across the world that it can be slow. In order to give the foreign country time to submit a mutual legal assistance request to obtain data relevant to an investigation, the Convention requires that a foreign preservation order would apply for a minimum of 60 days, pending the receipt of a mutual assistance request, as opposed to 20 days for domestic preservation orders.<sup>6</sup>

Crown Law has indicated that it can, in some cases, take six to 18 months for the formal mutual assistance process to be completed, which means that the initial 60-day period may need to be extended. This could be done upon judicial order, as many times as necessary, subject to certain criteria.<sup>7</sup>

**Question 6:** Would there be any difficulties with keeping preserved data for different periods depending on whether the order comes from a domestic or foreign source? What procedural or other changes would you need to make to do this?

**Question 7:** Would complying with a foreign order that is extended multiple times cause any challenges?

## Forward-looking preservation orders

The preservation of historic data ('retrospective preservation') would be the most important to preserve for law enforcement purposes, because these agencies' focus is more likely to be on events that have occurred in the past (i.e. when a crime has been committed).

However, in some circumstances, the behaviours of the alleged offender or victim after the criminal incident may also be relevant to law enforcement, in which case a 'prospective' data preservation order could be used for data that comes into the possession of the provider after they have received the order. One way this could work is an obligation on the recipient of the order to provide a series of 'one-off' preservation requests (e.g. 'take a regular snapshot of an email account on these particular dates'). This would help to conceptually separate prospective preservation orders from surveillance device warrants.

We are interested in what challenges and/or cost implications prospective preservation would create, and what would be required to allow this to happen. We note that:

- The Convention does not require prospective preservation. However, a number of overseas jurisdictions, including Australia, have adopted prospective preservation data retention schemes.

---

<sup>5</sup> The Law Commission report made a similar recommendation, stating that "as a matter of principle, foreign countries should not have access to more extensive law enforcement powers in New Zealand than domestic agencies."

<sup>6</sup> The Law Commission has also recommended this time period.)

<sup>7</sup> This would comport with New Zealand's existing mutual assistance regimes and s 130 of the Criminal Proceeds Recovery Act.

- A regime that was purely retrospective could encourage law enforcement agencies to issue or obtain multiple data preservation orders during the course of an investigation, so that data being generated from day to day and stored for only short periods was not being lost.
- Production orders in New Zealand can require ongoing production of relevant materials while the order is in force.<sup>8</sup>

Prospective preservation could also be limited to specific types of data (e.g. only call-associated data), specific agencies (e.g. only Police), or specific offences (e.g. those that carry a possible sentence of 7 years or more).

**Question 8:** What are the key implementation issues for prospective preservation that would impact on costs? Would you need to make a high degree of infrastructural or process change to enable this?

**Question 9:** If data preservation orders were to have a prospective element, should they have additional limiting parameters (for example, should there be limits on the types of data that are able to be prospectively preserved)? What would the challenges in implementation be if there were / were not additional limiting parameters?

## Types of data to preserve

Some of the most important data for law enforcement purposes is metadata, location data, and content data. Other types of data could include 'traffic', subscriber, and billing data.

The Convention requires that preservation be "of specified computer data, including traffic data." Computer data is defined broadly, and so would include most (if not all) types of telecommunications data. (We would expect there to be only occasional preservation requests for the engineering/cell tower data.)

- Computer data is defined in the Convention as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function." This could include a wide range of types of data, and would apply whether or not these communications are successfully sent or received.
- Traffic data is defined in the Convention as "computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service" It could include also include data on what cell tower a mobile phone is using to connect to the network (this is similar to the definition

<sup>8</sup> Search and Surveillance Act 2012, s 71(2)(g).

of call-associated data in the Telecommunications (Interception Capability and Security) Act 2013 ("TICSA")).<sup>9</sup>

**Question 10:** What challenges might arise from only applying a preservation scheme to certain types of data (e.g. content data), within the existing framework for providing data to law enforcement? What procedural or other changes would you need to make?

**Question 11:** Looking to future technological developments, will there be new types of data that would not fit within the envisioned categories described above? What are the challenges in retrieving or preserving these types of data?

## Penalties for non-compliance with a preservation order

The Law Commission report recommends that non-compliance with a preservation notice should be an offence, without specifying a penalty of a dollar amount or imprisonment term.<sup>10</sup>

A starting point for comparison could be production orders. The penalty for failing to comply with a production order is up to one year's imprisonment for an individual or, in the case of a body corporate, to a fine not exceeding \$40,000.<sup>11</sup>

Preservation orders could be seen as a 'lower level' type of order than production orders. However, vital data could still be lost if preservation orders are not complied with properly, which could have ongoing adverse implications for law enforcement outcomes.

**Question 12:** Should the maximum penalty for failing to comply with a preservation order be equivalent to the penalty for failing to comply with a production order? Why/why not?

---

<sup>9</sup> See section 3 of TICSA

<sup>10</sup> Recommendation 53.

<sup>11</sup> Search and Surveillance Act 2012, s 174.



## PART II: COSTS AND FUNDING OF A DATA PRESERVATION REGIME

Part II seeks feedback on the different types of costs to telecommunications companies of a data preservation regime, and seeks to quantify these costs. It then seeks initial thoughts on the allocation of these costs.

### Categories of costs

It is our understanding that prospective costs would fall into four categories:

- Additional time and resources spent on receiving and checking an order.
- Additional infrastructure to hold stored data, if this would be necessary.
- Processing capacity to copy and store the data.
- Other compliance and staffing costs.

**Question 13:** Do you agree with our above assessment of the categories of prospective costs? What other categories of costs might be incurred by compliance with a data preservation regime, if any?

### Quantifying costs

The parameters of a data preservation regime, as discussed in Part 1 of this document, are:

- Duration of preservation.
- Forward-looking preservation orders.
- Types of data to preserve.
- Penalties for non-compliance with a preservation order.

As mentioned above, New Zealand Police already contribute to the costs of telecommunications companies complying with these orders, currently funding 5,000 – 6,000 production order enquiries per annum with the three main telecommunications operators. Therefore, only the incremental costs of preservation orders will be relevant – excluding the costs that industry already incurs when complying with other types of law enforcement orders.

#### Number of orders

We are interested in how the number of preservation orders received might affect costs. Formalising a data preservation regime and allowing other nations to access it would likely mean the number of preservation orders increases.

We do not expect the number of data preservation requests to be high (approximately 30 per annum). However, we are seeking views on how the difficulties, costs, and cost-benefit analyses of

complying with the scheme would change at various intervals (including upper and lower extremes) of the possible number of requests received.

**Question 14:** How would increasing the number of preservation orders impact the difficulty of carrying them out? What changes would you have to make to your processes, infrastructure etc. to be able to do so?

*Please answer this question with reference to specific numbers of requests: e.g. for 2, 10, 30, 50, 100, 500, 5000, 10,000 preservation requests received, how would difficulties, costs, and cost-benefit analyses change?*

**Question 15:** Please list any other parameters of a data preservation regime that could have a cost impact.

**Question 16:** Please provide a general comment on which parameters would have the greatest and smallest cost impacts and why.

**Question 17:** Please provide some estimates of the costs that would be incurred by a data preservation regime. Give the lowest and highest bounds, allowing for variances in the above parameters (e.g. the total cost for a data preservation regime with retrospective preservation would be X, but with prospective preservation would be Y). If possible please provide detailed breakdowns of costs.

## Allocation of costs

The Convention does not comment on the allocation of data preservation regime costs between government and industry. New Zealand Police currently funds 5,000 – 6,000 production order enquiries per annum with the three main telecommunications operators under current arrangements in TICSAs. We are seeking views as to what cost allocations should govern a data preservation regime, and whether the current TICSAs arrangements provide the best structure.

Under current arrangements in TICSAs,<sup>12</sup> telecommunications companies are responsible for providing the infrastructure to enable interception and seizure of data, but law enforcement reimburses the cost of the extraction of data in individual cases. If the telecommunications company materially prejudices the investigation through non-compliance with TICSAs, law enforcement does not have to pay for the costs of interception. Disputes are resolved by mediation or arbitration.

**Question 18:** We seek initial views on the appropriate funding allocation scheme for data preservation.

**Question 19:** If the TICSAs regime is used as a starting point, how it would apply in the data preservation context? Would there be any differences or difficulties?

---

<sup>12</sup> ss 114-117.

## Full list of questions

Question 1: Would there be any challenges in preserving the data for 20 days? What would these be?

Question 2: How would extending the time period for preservation orders impact the difficulty of being able to carry them out?

Question 3: Would an extension of the order cause any additional challenges?

Question 4: Should legislation specify that preservation orders be discontinued if no longer applicable? Why/why not?

Question 5: After a preservation order ends, should data be destroyed when a notice is received? What procedural challenges could this create?

Question 6: Would there be any difficulties with keeping preserved data for different periods depending on whether the order comes from a domestic or foreign source? What procedural or other changes would you need to make to do this?

Question 7: Would complying with a foreign order that is extended multiple times cause any challenges?

Question 8: What are the key implementation issues for prospective preservation that would impact on costs? Would you need to make a high degree of infrastructural or process change to enable this?

Question 9: If data preservation orders were to have a prospective element, should they have additional limiting parameters (for example, should there be limits on the types of data that are able to be prospectively preserved)? What would the challenges in implementation be if there were / were not additional limiting parameters?

Question 10: What challenges might arise from only applying a preservation scheme to certain types of data (e.g. content data), within the existing framework for providing data to law enforcement? What procedural or other changes would you need to make?

Question 11: Looking to future technological developments, will there be new types of data that would not fit within the envisioned categories described above? What are the challenges in retrieving or preserving these types of data?

Question 12: Should the maximum penalty for failing to comply with a preservation order be equivalent to the penalty for failing to comply with a production order? Why/why not?

Question 13: Do you agree with our above assessment of the categories of prospective costs? What other categories of costs might be incurred by compliance with a data preservation regime, if any?

Question 14: How would increasing the number of preservation orders impact the difficulty of carrying them out? What changes would you have to make to your processes, infrastructure etc. to be able to do so?

*Please answer this question with reference to specific numbers of requests: e.g. for 2, 10, 30, 50, 100, 500, 5000, 10,000 preservation requests received, how would difficulties, costs, and cost-benefit analyses change?*

Question 15: Please list any other parameters of a data preservation regime that could have a cost impact.

Question 16: Please provide a general comment on which parameters would have the greatest and smallest cost impacts and why.

Question 17: Please provide some estimates of the costs that would be incurred by a data preservation regime. Give the lowest and highest bounds, allowing for variances in the above parameters (e.g. the total cost for a data preservation regime with retrospective preservation would be X, but with prospective preservation would be Y). If possible please provide detailed breakdowns of costs.

Question 18: We seek initial views on the appropriate funding allocation scheme for data preservation.

Question 19: If the TICSAs scheme is used as a starting point, how it would apply in the data preservation context? Would there be any differences or difficulties?





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

# Briefing

## BUDAPEST CONVENTION: LEGISLATION BID

To Minister of Broadcasting, Communications and Digital Media (Hon Faafoi)			
Date	27/11/2019	Priority	Routine
Deadline	29/11/2019	Briefing Number	1920NSP/034

### Purpose

To seek your agreement to signal your support for the Minister of Justice's bid for legislation to implement the requirements of the Budapest Convention in your legislative priorities letter for 2020.

### Recommendations

1. **Note** the attached bid for an omnibus bill to implement the domestic legislative requirements of the Budapest Convention (Attachment A) **NOTED**
2. **Note** that the bill would have a proposed priority of 9(2)(f)(iv) **NOTED**
3. **Agree** to signal your strong support for the bid in your legislative priorities letter for 2020 **YES / NO**

6(a)

PP

Sophie Vickers  
Team Manager, National Cyber Policy  
Office, National Security Policy  
Directorate

27/11/19

Hon Kris Faafoi  
Minister of Broadcasting,  
Communications and Digital Media

...../...../.....

BUDAPEST CONVENTION: LEGISLATION BID

Report No.  
1920NSP/034

## Contact for telephone discussion if required:

Name	Position	Telephone		1st contact
Sophie Vickers	Team Manager, National Cyber Policy Office	9(2)(a)	9(2)(a)	✓
6(a)	Principal Advisor, Cyber Security Policy	DDI	9(2)(a)	

## Minister's office comments:

- ☐ Noted
- ☐ Seen
- ☐ Approved
- ☐ Needs change
- ☐ Withdrawn
- ☐ Not seen by Minister
- ☐ Overtaken by events
- ☐ Referred to

# BUDAPEST CONVENTION: LEGISLATION BID

## Purpose

1. You and the Minister of Justice have signalled your intention to take a joint paper to Cabinet seeking agreement to accede to the Council of Europe Convention on Cybercrime (the Budapest Convention). In order to accede, domestic legislation would be required to bring New Zealand's laws into line with the requirements of the Convention.
2. To progress the development of legislation within the coming year, Ministers are required to submit legislative bids by 29 November for consideration by the Cabinet Legislation Committee. The Minister of Justice intends to submit a bid for legislation that would implement the requirements of the Budapest Convention. This paper summarises the approach to the bid, which is included at Attachment A.

## Domestic legislation is required for accession

3. The Budapest Convention makes international cooperation on cybercrime easier, by harmonising national laws on cybercrime and cyber-enabled crime, improving investigative techniques, and increasing international law enforcement cooperation.
4. In order to accede, parties must ensure their laws are aligned with the requirements of the Budapest Convention. New Zealand's laws are largely already in line, but a small number of changes will be needed [briefing DPMC-2017/18-1377 outlines the required legislative changes in detail].
5. In summary, changes would be required to the Search and Surveillance Act 2012, the Mutual Assistance in Criminal Matters Act 1992 and the Crimes Act 1961. All three Acts are administered by the Ministry of Justice. The attached legislative bid proposes an omnibus bill be presented to Parliament to:
  - a) introduce data preservation orders (which would require entities that hold specific information relevant to a specific criminal investigation to preserve that information temporarily, while a production order is sought)
  - b) introduce third party confidentiality orders (requiring third parties who are aware of the execution of a surveillance device warrant or preservation order to keep this confidential to protect investigations)
  - c) make adjustments to New Zealand's domestic mutual assistance law, to add surveillance device warrants and production orders to our mutual assistance regime
  - d) make minor changes to some elements of our computer crime offences.
6. In addition, an Order in Council would be promulgated under either the Customs and Excise Act 2018 or the Imports and Exports (Restrictions) Act 1988 to prohibit the intentional import of hardware for a computer crime.



9(2)(f)(iv)

7. 9(2)(f)(iv)

8. While early legislation is desirable to progress accession as quickly as possible, we will be able to begin to realise some of the benefits of membership before the legislation is passed. If Cabinet approves accession, the Minister of Foreign Affairs will write to the Council of Europe Secretariat with a request for accession. The Council would respond with an invitation to accede, which would enable New Zealand to have 'observer status' including the ability to attend Convention meetings. This would include negotiations on the second additional protocol to the Convention (covering cross-border access to evidence)<sup>6(b)</sup>

## Next Steps

9. Cabinet Office will compile all the legislative proposals and submit them to the Cabinet Legislation Committee for a decision on which bills are to be included in the Legislation Programme, and the priority that they will be given.
10. We will provide advice by 5 December on the proposed approach to targeted consultation to inform Cabinet's consideration of accession.

Attachments:	
Attachment A:	Accession to the Council of Europe Convention on Cybercrime (the Budapest Convention) Bill: Request for Priority in the 2020 Legislation Programme.



## ATTACHMENT A

Accession to the Council of Europe Convention on Cybercrime (the Budapest Convention) Bill: Request for Priority in the 2020 Legislation Programme

[SEPARATE DOCUMENT]

Released under the Official Information Act 1982

In Confidence

Office of the Minister of Justice

Cabinet Legislation Committee

**Accession to the Council of Europe Convention on Cybercrime (the Budapest Convention)****Bill: Request for Priority in the 2020 Legislation Programme****Summary information**

- 1 Give the following details about the bid for legislation:
  - 1.1 the portfolio of sponsoring Minister; Justice;
  - 1.2 the department responsible: Ministry of Justice (contact Lauren McIntosh, Policy Manager, Criminal Law, Ministry of Justice, 04 494 1084);
  - 1.3 the title of the proposed Bill: Accession to the Council of Europe Convention on Cybercrime (the Budapest Convention) Bill
  - 1.4 the proposed ranking of Bill within the bids from this portfolio: 18 of 20;
  - 1.5 the estimated size and complexity: medium size and of medium complexity; and
  - 1.6 the proposed priority: 9(2)(f)(iv)
- 2 The Accession to the Council of Europe Convention on Cybercrime Bill would bring New Zealand law in line with the legislative requirements of the Budapest Convention prior to accession. Changes would be made to the Search and Surveillance Act 2012, the Mutual Assistance in Criminal Matters Act 1992, and the Crimes Act 1961, as well as promulgation of an Order in Council under the Customs and Excise Act 2018 or the Imports and Exports (Restrictions) Act 1988, as described below.


**Policy**

- 3 Cybercrime is difficult to mitigate due its borderless nature. Harm can include fraud and theft, identity theft, and the online publishing of child exploitation material and terrorist content. This harm can come from criminals outside New Zealand who target New Zealanders, and from New Zealanders committing crimes online in other countries.
- 4 The Council of Europe Convention on Cybercrime (the Budapest Convention) is a treaty that enables international co-operation on cybercrime. While the Convention is a Council of Europe instrument, it is open to all states to accede by invitation.
- 5 Accession to the Budapest Convention would enable broader access to information sharing on current threats and best practice to better aid law enforcement. It would provide New Zealand agencies easier access to data to help prevent, mitigate, investigate and prosecute cybercrime by and against New Zealanders. It would also increase international law enforcement co-operation, and the opportunity to engage in negotiations on future

agreements to ensure New Zealand's interests are represented. Accession would increase New Zealand's contribution to fighting cybercrime globally.

- 6 Accession to the Convention would have significant reputational value for New Zealand. It would demonstrate support for best practice standards established by the Convention, and broader support for a rules-based international order. Accession is a key priority in New Zealand's Cyber Security Strategy 2019 [CAB-18-MIN-0127].
- 7 Legislative changes are required to bring New Zealand law in line with the Budapest Convention prior to accession. Changes would be presented to Parliament in detail as an omnibus Bill. They include:
  - 7.1 data preservation orders (which would require entities that hold specific information relevant to a specific criminal investigation to preserve that information temporarily, while a production order is sought);
  - 7.2 third party confidentiality orders (requiring third parties who are aware of the execution of a surveillance device warrant or preservation order to keep this confidential to protect investigations);
  - 7.3 adjustments to New Zealand's domestic mutual assistance law; and
  - 7.4 minor changes to some elements of our computer crime offences.
- 8 In addition, an Order in Council would be promulgated under either the Customs and Excise Act 2018 or the Imports and Exports (Restrictions) Act 1988 to prohibit the intentional import of hardware for a computer crime. This is also required in order to accede.
- 9 Cabinet approval is required for agreement for New Zealand to accede to the Budapest Convention. The Minister of Broadcasting, Communications and Digital Media and I will jointly take a paper to Cabinet in early 2020. Accession is subject to the satisfactory completion of the Parliamentary treaty examination process and implementation of necessary legislation.

#### **Need for legislation**

- 10 Legislation is required in order to meet the domestic legislative requirements of the Budapest Convention by its party members prior to accession.
- 11 The proposed priority of the Bill is 9(2)(f)(iv)  

- 12 Amendments have been made within the last year to the Crimes Act 1961 to introduce a new offence and repeal another. These amendments are unrelated to this proposal. The other pieces of legislation captured in this Bill have not been amended recently.

#### **Compliance**

- 13 The Bill is expected to comply with each of the following:
  - 13.1 the principles of the Treaty of Waitangi;

- 13.2 the rights and freedoms contained in the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993;
- 13.3 the principles and guidelines set out in the Privacy Act 1993;
- 13.4 the relevant international standards and obligations; and
- 13.5 the *Legislation Guidelines (2018 edition)*, which are maintained by the Legislation Design and Advisory Committee.

*The principles of the Treaty of Waitangi*

- 14 The Crown has a responsibility to inform Māori of upcoming developments in international law. The Convention touches upon issues of significance for Māori, including international relations, the justice system, search and surveillance, human rights and data sovereignty.
- 15 Data preservation orders, such as those required under the Budapest Convention, would require entities that hold data, that is in danger of being lost, to preserve it temporarily on their systems, while a production order is sought. As this tool would be used in relation to a variety of data types, acknowledgement should be made of the rights guaranteed under the Treaty in which Māori have rangatiratanga over their data.
- 16 The legislative requirements of the Budapest Convention require the addition of third party confidentiality orders for surveillance device warrants and preservation orders. These orders would require third parties aware of the order to keep that knowledge confidential. The addition of third party confidentiality for surveillance device warrants and preservation orders may raise concerns, in the context of perceptions that search and surveillance powers have been used disproportionately against Maori.
- 17 In order to better understand and mitigate the issues raised in this Treaty analysis section, officials would undertake targeted consultation with Māori before any legislation is developed. This consultation would ensure that Māori with an interest in international relations, the justice system, search and surveillance, privacy, and data sovereignty would be provided the chance to identify the Māori interests in these proposals and how they might best be protected. This would help guide the development of legislation. I consider this to be an important means to engage with Māori and ensure that their voice is represented if this work were to progress.
- 18 Reference should also be made to the Wai 262 report which discusses Treaty principles in relation to international instruments. This chapter discusses past engagement with Māori in relation to international instruments such as the Agreement on Trade-Related Aspects of International Property Rights, as well as the framework that the Crown has used to engage with Māori. I consider it important for this proposal to acknowledge this history of engagement with Māori when negotiating or considering accession to international instruments, such as the Budapest Convention.

*New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993*

- 19 Some legislative changes required for accession have human rights implications. Data preservation orders require consideration of section 21 of the New Zealand Bill of Rights Act, which addresses protection against unreasonable search and seizure. Preserving an individual's data could be perceived to impose upon this.



- 20 However, data preservation orders would only preserve a discrete ‘snapshot’ of data. They would be narrow in scope and are already held by a service provider in the normal course of business. The criteria to issue a data preservation order would be stringent enough to ensure that rights are not unduly imposed upon.
- 21 Extending third-party confidentiality to data preservation orders, and surveillance device warrants also requires consideration of sections 21 – 27 of the New Zealand Bill of Rights Act, which address search, arrest, and detention. This is because individuals would be unaware that their data was being stored or accessed by enforcement agencies.
- 22 However, these sections require the person to be informed only where a charge is laid. Data preservation orders, and surveillance device warrants are used at the early, evidence-gathering stage of an investigation. The former does not allow data to be handed over. The latter is only available for very serious offending. Once evidence has been gathered using these tools, the person would be informed if a charge were to be laid.
- 23 I believe all legislative changes are justifiable and sufficiently safeguarded. New Zealand law has multiple safeguards in place for various criminal offences and law enforcement powers. These protections would apply to the legislative changes required to accede to the Convention, including where other countries use them through the mutual assistance process. These safeguards include judicial authorisation for search warrants and production orders, and human rights provisions in mutual assistance laws.
- 24 There are general provisions on human rights in the Budapest Convention, which all states party must adhere to. These cover due process, territorial sovereignty, and requiring human rights protections of states party, and are broadly echoed in New Zealand law.

### **Binding on the Crown**

- 25 This Bill will be binding on the Crown.

### **Consultation**

- 26 The Ministry of Justice and the Department of the Prime Minister and Cabinet are jointly leading this project.

#### *Public consultation*

- 27 Accession to the Budapest Convention is included as a key area of focus in the New Zealand Cyber Security Strategy 2019. The strategy was widely consulted. Officials engaged with stakeholders from a range of non-government and private sector organisations and the public through workshops, an online feedback form, and discussion groups in Auckland, Wellington and Christchurch. Over 200 participants from all sectors joined these discussion groups. Overall, there was clear and strong support for accession.
- 28 The Law Commission and the Ministry of Justice undertook extensive public consultation as part of their joint review of the Search and Surveillance Act 2012, including on the possible introduction of a data preservation scheme and acceding to the Budapest Convention. The resulting report recommended that the Government consider accession to the Budapest Convention. The report also set out suggested parameters for a data preservation scheme which officials are taking into account in the detailed policy design of the scheme.
- 29 Officials propose carrying out further targeted consultation before beginning work on legislative development. This further consultation would be a means for officials to work,

particularly with Māori, to ensure that the legislative changes are in line with public interests.

- 30 There will be further opportunities for public consultation and scrutiny through the Select Committee process. Select Committees will take public submissions on Convention accession during the Parliamentary treaty examination process; and on the specific legislative changes required during the passage of implementing legislation.

*Telecommunications companies and other affected parties*

- 31 Telecommunications companies and other affected parties, and law enforcement agencies, were consulted on the parameters of a data preservation scheme. 9(2)(ba)(i)

*Government Agencies*

- 32 This paper was prepared by the Department of the Prime Minister and Cabinet and the Ministry of Justice. The following departments have been consulted in preliminary policy work and preparation for Cabinet discussions: Crown Law; Department of Internal Affairs; Ministry of Business, Innovation and Employment; Ministry of Foreign Affairs and Trade; Ministry for Primary Industries; New Zealand Customs Service; New Zealand Police; the Serious Fraud Office; The Treasury; Te Arawhiti; and Te Puni Kōkiri. The Office of the Privacy Commissioner has also been consulted.

**Associated regulations**

- 33 No regulations will be needed.

**Timeline**

- 34 The proposed timing for the legislation is:

<i>Step</i>	<i>Proposed date</i>	<i>Consistency assurance</i>
Date on which final policy approvals were, or will be, obtained from Cabinet.	1 May 2020	-
Date on which final drafting instructions were or will be sent to the Parliamentary Counsel Office or other drafter.	9(2)(f)(iv)	
Date by which the Bill will be released for exposure draft (if an exposure draft is planned).	-	
Date by which the Bill will be provided to the Ministry of Justice (or the Crown Law Office if applicable) for an	9(2)(f)(iv)	

assessment of consistency with the New Zealand Bill of Rights Act 1990.		
Dates on which the Bill will be before LEG and Cabinet for approval for introduction.	9(2)(f)(iv)	
Date by which any policy decisions for associated regulations will be before Cabinet.	-	
Date requested for introduction of the Bill.	9(2)(f)(iv)	
Date of report back from select committee.	9(2)(f)(iv)	
Date on which final policy approvals will be obtained from Cabinet for any substantive SOP to Bill (if already introduced)	-	
Date on which final drafting instructions were or will be sent to the Parliamentary Counsel Office or other drafter for any substantive SOP to Bill (if already introduced).	-	
Date by which final drafting instructions for any associated regulations will be sent to the Parliamentary Counsel Office.	-	
Date of enactment.	9(2)(f)(iv)	
Date of commencement.	9(2)(f)(iv)	

## Recommendations

35 The Minister of Justice recommends that the Committee:

- 35.1 **note** that the Accession to the Council of Europe Convention on Cybercrime (the Budapest Convention) Bill will implement legislation required by the articles of the Budapest Convention;
- 35.2 **approve** the inclusion of the Accession to the Council of Europe Convention on Cybercrime (the Budapest Convention) Bill in the 2020 Legislation Programme, with a priority 9(2)(f)(iv) ;
- 35.3 **note** that drafting instructions will be provided to the Parliamentary Counsel Office 9(2)(f)(iv) ;
- 35.4 **note** that the Bill should be introduced no later than 9(2)(f)(iv) ;
- 35.5 **note** that the Bill should be passed no later than 9(2)(f)(iv) .

Authorised for lodgement

Hon Andrew Little  
Minister of Justice

~~IN CONFIDENCE~~

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

# Briefing

## TARGETED ENGAGEMENT ON ACCESSION TO THE BUDAPEST CONVENTION

To Minister of Justice (Hon Little)			
Minister of Broadcasting, Communications and Digital Media (Hon Faafoi)			
Date	9/12/2019	Priority	Routine
Deadline	13/12/2019	Briefing Number	DPMC: 1920NSP/035

### Purpose

This briefing seeks your agreement to carry out targeted consultation on accession to the Budapest Convention prior to taking a paper to Cabinet. This is in order to gain a better understanding of Māori interests in accession as well as any human rights, criminal and privacy law, and technology implications.

### Recommendations


1. **Agree** that officials will conduct targeted consultation with Māori on accession to the Budapest Convention YES / NO
2. **Agree** that officials engage with stakeholders with an interest in human rights, criminal and privacy law and technology to discuss accession to the Budapest Convention YES / NO
3. **Agree** to the use of the attached summary of the Budapest Convention and the necessary changes to New Zealand laws, to support engagement YES / NO
4. **Agree** to the proactive release of this briefing and its attachment following Cabinet's decision on the accession to the Budapest Convention YES / NO


TARGETED ENGAGEMENT ON ACCESSION TO THE BUDAPEST CONVENTION

Report No. DPMC: 1920NSP/035



IN CONFIDENCE

 <b>Lauren McIntosh</b> <b>Policy Manager, Criminal Law</b> <b>Ministry of Justice</b>	    <b>Hon Andrew Little</b> <b>Minister of Justice</b>
9/12/19	...../...../.....

<b>6(a)</b>  <b>Sophie Vickers</b> <b>Team Manager, National Cyber Policy</b> <b>Office</b> <b>Department of Prime Minister and</b> <b>Cabinet</b>	    <b>Hon Kris Faafoi</b> <b>Minister of Broadcasting,</b> <b>Communications and Digital Media</b>
9/12/19	...../...../.....

## Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Lauren McIntosh	Policy Manager, Criminal Law, Ministry of Justice	9(2)(a)	✓
9(2)(a)	Policy Advisor, Criminal Law, Ministry of Justice	9(2)(a)	
Sophie Vickers	Team Manager, National Cyber Policy Office, DPMC	9(2)(a)	✓
6(a)	Principal Advisor, Cyber Security Policy, DPMC	9(2)(a)	

## Minister's office comments:

- ☐ Noted
- ☐ Seen
- ☐ Approved
- ☐ Needs change
- ☐ Withdrawn
- ☐ Not seen by Minister
- ☐ Overtaken by events
- ☐ Referred to

# TARGETED ENGAGEMENT ON ACCESSION TO THE BUDAPEST CONVENTION

## Background

1. The Council of Europe Convention on Cybercrime (the Budapest Convention) aims to make international cooperation on cybercrime easier, by harmonising national laws on cybercrime and cyber-enabled crime, improving investigative techniques, and increasing international law enforcement cooperation.
2. You (Ministers Little and Faafoi) have signalled your intention to take a joint paper to Cabinet seeking agreement to accede to the Budapest Convention (briefing DPMC-2017/18-1377 refers). In November 2019, you (Minister Faafoi) agreed to delay a Cabinet discussion to February 2020, to allow time for targeted engagement ahead of a decision. This briefing sets out a proposed model for that engagement.

## There has been broad consultation on the principle of accession and targeted consultation on the design of a data preservation scheme

3. Accession to the Budapest Convention is included as a key area of focus in the New Zealand Cyber Security Strategy 2019, as well as being a priority within the post-Christchurch Countering Violent Extremism Online work programme. Accession is also linked to and would support the Government Cloud programme, including efforts to have major cloud providers establish facilities in New Zealand.
4. Previous engagement on the Budapest Convention has included consultation on the Cyber Security Strategy, as well as extensive public consultation on the Law Commission and Ministry of Justice review of the Search and Surveillance Act 2012. The resulting report recommended that the Government consider accession to the Budapest Convention. Further to this, in early 2019, officials consulted with telecommunications companies on the parameters of a data preservation scheme and its financial implications.
5. There has been an extensive period of engagement with Crown agencies on the development of the proposal to accede.<sup>9(2)(f)(iv)</sup>

## We propose a targeted approach to Māori engagement

6. The Cabinet-mandated 2001 Strategy for Engagement with Māori on International Treaties outlines how agencies will ensure that issues of relevance to Māori interests in international treaties are identified early. Lead agencies have responsibility for establishing appropriate engagement with Māori, based on the nature, degree and strength of Māori interest. The recent Te Tiriti o Waitangi guidelines agreed by Cabinet support agencies in considering the Treaty in policy development and implementation. The Waitangi Tribunal has also offered guidance, in particular through the report on the Wai262 claim, which reinforces the importance of engagement with Māori when



considering the making of or signing up to international agreements. The approach proposed in this paper draws on that body of guidance.

7. Officials consider it prudent to engage with Māori prior to seeking Cabinet approval to accede to the Convention, as there are areas where Māori may have an interest, including New Zealand's international obligations, the justice system, search and surveillance, human rights and data sovereignty. We do not consider this analysis to be complete and so engagement is necessary to allow an opportunity for Māori interests to be raised and ensure that these interests are fully understood, so that Cabinet may take this information into account in its decision-making.
8. The specific objective of this engagement would be to provide an opportunity for Māori to articulate and discuss Māori interests in the Budapest Convention, and how those interests might best be protected. To do this, we propose that DPMC and MOJ jointly host a hui in Wellington. Subject to your agreement, this would take place in the week of either 13 January or 20 January, subject to securing sufficient participation from attendees.
9. Noting the breadth and depth of diversity in communities and Māori, we propose to invite a small group of people (up to 12 guests) who can represent a wide range of views. A proposed invite list is attached at Annex A. We acknowledge however that it is not possible for one person or group of people to represent all Māori or all Māori viewpoints. Attendees from government agencies would be similarly limited in number and sufficiently senior to reflect the mana of invitees.
10. We would not seek to limit the scope of discussion, so that all interests could be raised, however we anticipate discussion would be likely to focus on data sovereignty in the criminal justice context, implications for Māori technology companies, as well as experience Māori have had in relation to the Crown's engagement with Māori when negotiating international agreements.
11. The costs for travel and kai would be met from DPMC baselines and are expected to be between \$5,000 to \$10,000.

### **There are some risks associated with a targeted approach to Māori consultation**

12. To meet the deadline of February 2020 for Cabinet consideration, the proposed approach to consultation is limited to a small number of people. This risks a limited group of experts being used as a proxy for a longer programme of engagement with iwi and hapū as a Treaty partner. This approach may also risk not all views being heard on the detail of implementation. We propose that the initial engagement acts as the start of a dialogue, and to be clear that there will be further consultation on the domestic implementation of the Convention.
13. If the hui suggests that the level of Māori interest is high, with multiple matters requiring further exploration and discussion, or if we are unable to gather a range of views in the time available, we will provide further advice on the best way to proceed and any implications for the timetable or the approach to seeking Cabinet's agreement to accede.
14. The Government's work to develop a whole-of-government approach to dealing with the issues raised in the Wai 262 claim and resulting Waitangi Tribunal report may in time provide a fuller framework for how the Crown engages with Māori on international agreements such as the Budapest Convention.

## We also aim to meet with a number of wider stakeholders

15. We suggest initiating further discussion in order to engage wider stakeholders with interests in human rights, criminal and privacy law and technology. This would gather a broader range of perspectives on the implications of accession, to inform advice to Cabinet. It will also support us in future communications around accession and its benefits. This group could include:

• 9(2)(a)

•

•

•

•

•

•

•

•

•

•

•

## Communications

16. There will be no proactive public communications about the engagement to be undertaken, though we do not propose to impose any requirement about confidentiality. We will prepare reactive Q&A covering issues that may be raised and will share these with your office before the meetings start.
17. We propose to share a summary of the Budapest Convention and the changes that would be required to New Zealand's laws ahead of any meetings. This is attached at Attachment B for your review. This would be tailored for engagement with different stakeholders, to reflect the likely discussion. This version would be used for invitees to the hui.

## Next Steps

18. If you agree to the approach set out in this paper, we will make arrangements for the hui and seek meetings with our proposed consultees.
19. In parallel, we are continuing to engage with agencies to develop the narrative around accession and the Cabinet paper.

Attachments:	
Attachment A:	Provisional hui invite list
Attachment B:	Summary of Budapest Convention



## ATTACHMENT A: PROVISIONAL HUI INVITE LIST

9(2)(a)



## ATTACHMENT B: SUMMARY OF THE BUDAPEST CONVENTION FOR EXTERNAL USE

### COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

The Council of Europe Convention on Cybercrime (the Budapest Convention) is an international treaty aiming to address internet and computer crime. It was agreed in 2001.

The convention now has 64 members. New Zealand has not yet joined. A key focus of the New Zealand Cyber Security Strategy is to consider whether New Zealand should join the Convention. Government agencies have been working to understand the benefits of joining and the changes that would be required to New Zealand's laws.

We want to discuss this with you so that we can understand your views on the implications of joining the Convention. In support of the Crown's obligations under Te Tiriti o Waitangi, we want to understand Māori interests in this issue, and how those interests can be best protected, before Ministers take a decision whether to join.

#### **The Convention makes international cooperation on cybercrime easier**

Cybercrime frequently involves individuals or computer systems in more than one country. The harmful effects of cybercrime can come from criminals outside New Zealand who target New Zealanders, and from New Zealanders committing crimes online in other countries. Investigations often rely on information and evidence held overseas. International cooperation on cybercrime is essential in investigations and prosecutions.

The Budapest Convention helps with this by:

- aligning national laws on cybercrime, so that the same action would be a crime in all countries.
- improving techniques for investigations, to make it easier to get evidence needed to investigate crimes. This includes the ability to order companies to store or provide specific data, including data about or owned by their customers.
- increasing international law enforcement cooperation, such as sharing of evidence to help investigations.

#### **Member states must align their laws and commit to cooperate**

Member states must bring their laws into line with the Convention requirements before joining. Members commit to cooperating on criminal investigations related to computer systems and data, and on the collection of electronic evidence of a criminal offence.

#### **Joining would have benefits for New Zealand**

Membership of the Convention would help prevent, investigate and prosecute cybercrime by and against New Zealanders, through:

- better access to information on cybercrime threats and the latest techniques for tackling them
- making it easier to obtain overseas data that agencies need for criminal investigations, and to participate in investigations involving multiple countries
- reducing reliance on voluntary assistance from other countries and overseas companies.



It would also mean New Zealand would be able to participate in negotiations on future international law on cybercrime, ensuring our interests are protected. Better laws for investigating cybercrimes would encourage confidence in New Zealand's cyber environment and support investment by businesses.

Joining the Convention would improve New Zealand's international reputation, because it signals New Zealand takes cybercrime seriously and supports established, lawful methods for investigating crime.

## **A number of changes would be required to New Zealand laws**

New Zealand laws already align with most of the Convention requirements, through the Crimes Act 1961, the Mutual Assistance in Criminal Matters Act 1992 and the Search and Surveillance Act 2012. New legislation would be needed to:

- introduce data preservation orders. These would require people or organisations that hold specific information relevant to a specific criminal investigation to temporarily keep that information, in the gap before a legal order to provide that information is obtained. For example, the police could require a telecommunications company to temporarily hold on to text messages sent by an individual on a certain day, if they were likely to be relevant to a criminal investigation, until legal authority was granted to obtain them.
- introduce third party confidentiality orders. These would require anyone who is aware of the use of data preservation orders and warrants for electronic interception, tracking and recording to keep this confidential, to protect investigations. For example, this could mean that an internet company would be required to not tell an individual that they had been asked to hold on to some of their data for use in a criminal investigation.
- adjust our mutual assistance law. This would add two current investigative measures to our mutual assistance regime, so that agencies can cooperate effectively in international investigations. For example, this could mean that a New Zealand agency could use its legal powers to require an internet company to provide certain information, and share that information with a UK agency, to help them investigate a serious hacking in the UK.
- make a number of other minor amendments to relevant laws.

## **What we hope to discuss**

The He Waka Roimata report by Te Uepū Hāpai I te Ora, discussions on the Data Protection and Use Policy and the Māori Data Futures project provided much helpful feedback to inform government's policy work. These included concerns over Māori over-representation in the criminal justice system, the need for culturally-informed solutions to the problems of social harm and crime, that trust in government is a key issue and that data should be used with reference to Māori priorities, values and worldviews, among other matters. In that context, we want to discuss questions such as:

- Do you have a view on the proposal that New Zealand join the Budapest Convention?
- Do you see any opportunities or benefits for iwi, hapū or whanau?
- What are some of the Treaty/Māori interests in this issue, in your view?
- How may Māori interests be best protected?
- Is there anyone else that you think we should talk to before Ministers take a decision? What are the risks of joining without further consultation with iwi or hapū?

## What will happen next?

We will summarise what we have heard in our advice to Ministers. If the Government decides to go ahead, the Convention would be reviewed in Parliament by a Select Committee, who may invite people to submit views on whether New Zealand should join. There would be more opportunities to discuss these changes and how they are implemented before they became law.

Released under the Official Information Act 1982





# Briefing

## OPTIONS FOR CABINET CONSIDERATION OF ACCESSION TO THE BUDAPEST CONVENTION

To Minister of Broadcasting, Communications and Digital Media, Hon Kris Faafoi

Date	19/02/2020	Priority	Routine
Deadline	26/02/2020	Briefing Number	1920NSP/056

### Purpose

To seek your direction on timing for Cabinet consideration of New Zealand accession to the Budapest Convention.

### Recommendations

1. **Note** that seeking Cabinet agreement to accede to the Budapest Convention is a key area of focus in Cyber Security Strategy 2019, and a key deliverable in the countering violent extremism online and Government Cloud programmes.
2. **Note** the upcoming 6(b) Plenary on the Second Additional Protocol to the Budapest Convention will discuss cooperation on law enforcement access to evidence held in the cloud, the ability for law enforcement to cooperate directly with service providers in other countries, improved mutual legal assistance for electronic evidence, and safeguards including around data protection.
3. **Note** New Zealand's involvement in these discussions would send a strong signal New Zealand is serious about cooperating with other countries in combating cybercrime. 6(b)
4. **Note** for New Zealand to participate in the 6(b) Plenary with observer status, the Minister of Foreign Affairs would need to send a letter expressing interest in acceding to the Convention by early April 2020.



5. **Note** MFAT's advice that sending a letter would imply a political obligation analogous to the signing stage in the multilateral treaty negotiation process, and therefore requires Cabinet approval.

6. **Note** further engagement is required with Māori to assist with clarifying Māori interests in the Convention.

7. **Agree** to either

a. Option A (preferred option): a two stage process, seeking Cabinet agreement to send a letter requesting an invitation to accede to the Budapest Convention; and to formally engage with Māori and other interested parties on a draft National Interest Analysis document, by April 2020. A second paper would be presented to Cabinet in November 2020, requesting authorisation to accede following completion of Parliamentary Treaty Examination and passage of legislative and regulatory changes. New Zealand would attend the <sup>6(b)</sup> Plenary.

YES / NO

or:

b. Option B: a single stage process seeking Cabinet agreement to accede to the Budapest Convention following completion of Parliamentary Treaty Examination and passage of legislative and regulatory changes by mid-June 2020. This process would include further informal engagement with Māori and other interested stakeholders. New Zealand would not attend the <sup>6(b)</sup> Plenary.

YES / NO

or:

c. Option C: seek Cabinet approval for formal engagement with Māori and other interested parties on a draft National Interest Analysis in March 2020, followed by a single stage process seeking Cabinet agreement to accede to the Budapest Convention following completion of Parliamentary Treaty Examination and passage of legislative and regulatory changes by mid-June 2020. New Zealand would not attend the <sup>6(b)</sup> Plenary.

YES / NO

8. **Agree** to forward this briefing to the Minister of Justice, Minister of Foreign Affairs, and the Attorney General.

YES / NO

6(a)

Sophie Vickers  
Team Manager, National Cyber Policy  
Office, National Security Policy Directorate

Hon Kris Faafoi  
**Minster of Broadcasting,  
Communications and Digital Media**

19/2/20

...../...../.....

## Contact for telephone discussion if required:

Name	Position	Telephone		1st contact
Sophie Vickers	Team Manager, National Cyber Policy Office, National Security Policy Directorate	9(2)(a)	9(2)(a)	✓
6(a)	Senior Advisor, National Security Policy Directorate		9(2)(a)	

## Minister's office comments:

- ☐ Noted
- ☐ Seen
- ☐ Approved
- ☐ Needs change
- ☐ Withdrawn
- ☐ Not seen by Minister
- ☐ Overtaken by events
- ☐ Referred to

# OPTIONS FOR CABINET CONSIDERATION OF ACCESSION TO THE BUDAPEST CONVENTION

## Background

1. At the meeting with officials on Monday 10 February, you requested a paper outlining the various timeline options for Cabinet's consideration of accession to the Council of Europe Convention on Cybercrime (the Budapest Convention).
2. The Convention is the first, and currently only, international treaty seeking specifically to address Internet and computer crime. It deals with crimes committed via the Internet and other computer networks, particularly infringements of copyright, computer-related fraud, child pornography and violations of network security.
3. It does so by aligning national laws, facilitating information-sharing on current threats and best practice, increasing international law enforcement cooperation, and fostering international dialogue. Benefits of membership also include access to resources, training and tools that we might not otherwise have.
4. 6(a), 6(b)
5. Following attendance at the Quintet of Attorneys General in 2018 and 2019, the Attorney-General urged in his Report on Overseas Travel that New Zealand's accession to the Convention be fast tracked.

## Convention members are negotiating new provisions on cloud data

6. Parties to the Convention are currently negotiating a Second Additional Protocol to the Convention, relating to access to evidence in the cloud. The Additional Protocol is intended to enhance the efficiency of obtaining electronic evidence through mutual assistance. The scope of evidence addressed by the Additional Protocol is accordingly much wider than pure cybercrime.
7. Negotiations on the Protocol have been underway since 2017. However, we understand the next meeting in 6(b) in the following areas:
  - a) law enforcement access to electronic evidence in the cloud;
  - b) more effective mutual legal assistance processes;
  - c) direct cooperation between law enforcement and service providers; and
  - d) safeguards, including data protection requirements.
8. The current mutual legal assistance process is inefficient in general, and particularly so with respect to obtaining electronic evidence. There can be a 6 – 24 month response time for requests for electronic evidence from other countries, particularly the United States where companies such as Facebook and Microsoft are based. 6(b)



6(b)

9. 6(b)

10. 6(b)

11. Participation would send a strong signal New Zealand is serious about cooperating with other countries in combating cybercrime. It also reinforces New Zealand's commitment to the protection of human rights, including privacy protections and freedom of expression, represented by the Convention.

12. 6(a), 6(b)

In 2019, New Zealand signed the Quintet of Attorneys General's Statement on international cooperation on cybercrime in support of the Budapest Convention<sup>6(a)</sup>

13. In addition to law enforcement outcomes, participation in developing international regulatory frameworks and adoption of these is expected to be an important factor in facilitating investment in and development of cloud capability in New Zealand.

### **New Zealand needs an invitation to attend negotiations**

14. New Zealand can only participate in negotiations if it receives an invitation from the Council of Europe to accede to the Budapest Convention. 'Invited party' status would provide New Zealand with some immediate benefits ahead of accession, including sharing of best practice in relation to prevention and investigation techniques, and the ability to attend Convention meetings as an observer.<sup>6(b)</sup>

15. This process is initiated via a letter from New Zealand's Minister of Foreign Affairs to the Council of Europe Secretariat, expressing interest in accession to the Convention.<sup>6(b)</sup>

16. Invited party status lasts for five years (the 'on-ramp') after the Council's invitation to accede. If we have not acceded within those five years, the invitation lapses.

### **An invitation is akin to signing stage of a treaty negotiation process**

17. Sending a letter indicating our interest in accession does not have legal effect. But it does imply a political obligation – that New Zealand intends to accede – and triggers the first

<sup>1</sup> Quintet of Attorneys General, *Statement on international cooperation on cybercrime*, London, July 30-31, 2019.

step of the accession process. This is a policy decision analogous to the signing stage in the multilateral treaty negotiation process.

18. MFAT advises that a letter would require Cabinet approval, with the Cabinet paper setting out the likely measures needed to implement the Convention in New Zealand and seeking at least high-level 'in principle' policy decisions. MFAT does not think a final detailed policy decision to support the development of legislation is needed at this stage, but that Cabinet needs to be alerted to the likely legislative and policy implications that need to be considered, so it can make an informed decision to seek an invitation to accede.
19. A second Cabinet paper would then need to be submitted. This would include the text of the Convention, as well as a final National Interest Analysis, and would request authorisation to accede following completion of Parliamentary Treaty Examination and passage of legislative and regulatory changes.<sup>2</sup>
20. The normal process is to combine these two steps into a single paper. This was the approach officials had been following. However, given a need to engage further with Māori on the benefits and implications for Māori of accession, this paper provides both single and two-step process options to incorporate further engagement with Māori and other stakeholders, while moving as quickly as possible to provide advice to Cabinet on accession.

### **Further engagement with Māori is recommended before a final decision to accede**

21. The hui held to ascertain Māori interests in the Convention identified a number of issues which are relevant to a broader policy conversation in the cybersecurity area. DPMC will take forward those conversations as part of its overall approach to implementing the Cyber Security Strategy 2019.
22. The hui also highlighted the need for a better explanation of the implications of accession for New Zealand and Māori specifically. Clarification is also required in terms of the context of the Convention against the background of existing law enforcement and mutual assistance legislation. In practice, we believe the impact on Māori of changes required by accession to the Budapest Convention is likely to be very narrow. The majority of the powers required in order to accede to the Convention, such as search warrants, are already available under New Zealand law. However, feedback following the hui has confirmed that further engagement with Māori is recommended.

23. 9(2)(h)

Advice on accession to the Convention is also a

<sup>2</sup> Following Cabinet approval, the Convention text and the National Interest Analysis (NIA) would then be presented to Parliament for the treaty examination process. Once presented, the Government must refrain from taking binding treaty action until the relevant select committee has reported or fifteen sitting days have elapsed. If no recommendation requiring further government action is required, the parliamentary treaty examination process is complete when the select committee presents its report. Subject to agreement, implementing legislation would then be introduced to Parliament. If the legislation is passed, New Zealand can then deposit an Instrument of Accession with the Council of Europe. This would note any reservations or declarations. It would be signed and sealed by the Minister of Foreign Affairs.



key deliverable of the Cyber Security Strategy 2019, countering violent extremism online work programme, and the Government Cloud programme.

## Options for Cabinet consideration

24. The table below outlines three timing options for Cabinet consideration of accession to the Convention:
- a) **Option A: Two stage process** – Cabinet decision sought in March 2020 for approval to release the National Interest Analysis for public consultation and to write to the Council of Europe expressing interest in accession to the Convention. A second paper would be presented to Cabinet in June 2020, requesting authorisation to accede following completion of Parliamentary Treaty Examination and passage of legislative and regulatory changes.
  - b) **Option B: single stage process** – seeking Cabinet agreement by May 2020 to accede to the Budapest Convention following completion of Parliamentary Treaty Examination and passage of legislative and regulatory changes. This process would allow further informal consultation with Māori and other interested parties to inform a Cabinet decision on accession.
  - c) **Option C: Formal consultation followed by single stage process** – Cabinet approval for public consultation on a draft National Interest Analysis in March 2020, followed by a single stage process seeking Cabinet agreement to accede to the Convention following completion of Parliamentary Treaty Examination and passage of legislative and regulatory changes after the election.
25. Officials recommend Option A as this allows attendance at the <sup>6(b)</sup> meeting, while also allowing for public consultation. Officials believe risks of this option can be mitigated through careful communication with stakeholders.

Table 1: Options analysis

9(2)(g)(i)

Table content is redacted.

## Next Steps

---

26. Following your agreement to a preferred approach, officials will implement a work plan towards your preferred option and provide updates on progress via the weekly report and regular meetings with officials as required.
27. Officials will update Māori and other stakeholders on the direction of travel and how they can be involved in the process.

Attachments:	
Attachment A:	Detailed Timeline of Options A - C

## Attachment A - Detailed Timeline of Options

### Option A: Two Stage Process

**Description:** Paper to Cabinet Social Wellbeing Committee (SWC) meeting in March 2020 seeking approval to release the National Interest Analysis (NIA) for consultation and send a letter to the Council of Europe expressing interest in accession to the Convention. Second paper presented to Cabinet in June 2020, requesting authorisation to accede following completion of Parliamentary Treaty Examination and passage of legislative and regulatory changes.

Date	Action	Notes
<b>Following decision on timeline</b>	Hui participants informed of approach	Highlight that Cabinet approval would be sought for in principle decision to accede, subject to further engagement and treaty examination process
<b>Mon 24 Feb</b>	Draft Cabinet paper and NIA provided to Minister's office  Draft Cabinet paper and NIA distributed for agency consultation	
<b>Fri 28 Feb</b>	Draft papers incorporating agency feedback provided to Minister's office  Ministerial consultation on paper	
<b>Thu 12 Mar</b>	Lodge paper for SWC	
<b>Wed 18 Mar</b>	SWC Committee considers paper	Paper seeks approval to: <ul style="list-style-type: none"> <li>• Send letter expressing interest in acceding</li> <li>• Consult on the NIA document</li> </ul>
<b>Mon 23 Mar</b>	Cabinet considers paper	
<b>Tue 24 Mar</b>	Minister of Foreign Affairs signs letter following Cabinet approval  Consultation opens on the NIA	Letter will note New Zealand needs to complete internal policy processes, including engagement with Maori. Timing would allow attendance at 6(b) Plenary meeting.
<b>Tue 28 Apr</b>	Consultation closes on NIA	5 week consultation period on NIA
<b>Fri 1 May</b>	Draft Cabinet paper distributed for agency consultation	1 week consultation period (informal consultation prior)
<b>Thu 7 May</b>	Draft Cabinet paper provided to Minister's office	

<b>Thu 14 May</b>	Ministerial consultation on paper	2 week consultation period
<b>Thu 28 May</b>	Lodge paper for ERS	
<b>Tue 2 June</b>	ERS Committee considers paper	Paper seeks approval to accede to Budapest Convention following: <ul style="list-style-type: none"> <li>• completion of Parliamentary Treaty Examination</li> <li>• passage of legislative and regulatory changes</li> </ul>
<b>Mon 8 June</b>	Cabinet considers paper	
<b>Tue 9 June</b>	Drafting instructions issued	Ministry of Justice estimates the time required between instructions and introduction to the House is 8 – 10 weeks
<b>TBC</b>	Treaty examination process commences	
<b>TBC</b>	Legislation introduced	



## Option B: Single Stage Process

**Description:** Paper to Cabinet Social Wellbeing Committee (SWC) in May seeking Cabinet agreement to accede to the Budapest Convention following completion of Parliamentary Treaty Examination and passage of legislative and regulatory changes. This process would include further informal engagement with Maori. New Zealand would not attend the <sup>6(b)</sup> Plenary.

Date	Action	Notes
Mon 17 Feb – Mon 16 Mar	Further informal engagement with Maori and other stakeholders	One month further consultation period. (Consultation can continue until NIA review if required.) Other stakeholders will also be consulted.
Mon 16 Mar	Draft Cabinet paper and NIA distributed for agency consultation	2 week consultation period
Week 30 Mar	NIA review	Update and re-consult with agencies as required
Thu 9 Apr	Draft Cabinet paper and NIA provided to Minister's office	
Thu 16 Apr	Ministerial consultation on paper and NIA	2 week consultation period – note over Parliamentary recess
Thu 30 Apr	Lodge paper for SWC	
Wed 5 May	SWC Committee considers paper	Paper seeks approval to accede following: <ul style="list-style-type: none"> <li>• completion of Parliamentary Treaty Examination</li> <li>• passage of legislative and regulatory changes</li> </ul>
Mon 11 May	Cabinet considers paper	
Tue 12 May	Minister of Foreign Affairs signs letter expressing interest in accession following Cabinet approval	
Wed 13 May	Drafting instructions issued	Justice estimates the time required between instructions and introduction to the House is 8 – 10 weeks
TBC	Treaty examination process commences	
TBC	Legislation introduced	

### Option C: Formal consultation followed by single stage process

<b>Description:</b> Paper to Cabinet External Relations and Security Committee (ERS) in March seeking approval for formal engagement with Māori and other interested parties on a draft National Interest Analysis (NIA). Paper following seeking Cabinet agreement to accede to the Budapest Convention following completion of Parliamentary Treaty Examination and passage of legislative and regulatory changes. New Zealand would not attend the <sup>6(b)</sup> Plenary.		
Date	Action	Notes
Week 17 Feb	Draft Cabinet paper and NIA distributed for agency consultation	Less than 1 week consultation
Mon 24 Feb	Draft Cabinet paper and NIA provided to Minister's office  Ministerial consultation on paper and NIA	1.5 week consultation (if targeted SWC could extend consultation period)
Thurs 5 Mar	Lodge paper to ERS	
Tues 10 Mar	ERS Committee considers paper	
Mon 16 Mar	Cabinet considers paper	
Tues 17 Mar	Consultation on NIA	Long consultation process on the NIA  All prep for Cabinet decision occurs over this period (Cabinet paper, drafting instructions etc)
After 2020 Election	2 <sup>nd</sup> Cabinet paper with policy decisions following consultation is presenting to the incoming Government, send letter following Cabinet approval	

~~IN CONFIDENCE~~

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

# Briefing

## CABINET PAPER: IN-PRINCIPLE DECISION ON ACCESSION TO THE BUDAPEST CONVENTION

To Minister of Broadcasting, Communications and Digital Media (Hon Kris Faafoi)

Date	11/03/2020	Priority	Routine
Deadline	26/03/2020	Briefing Number	1920NSP/058

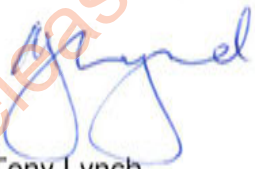
### Purpose

1. This note introduces the attached draft Cabinet paper for your consideration (Attachment A). The paper is seeking an in-principle decision for New Zealand to accede to the Council of Europe's Budapest Convention on Cyber Crime ("the Budapest Convention"). It is proposed that the Cabinet paper be taken to the Cabinet Social Wellbeing Committee on 1 April.
2. Speaking points are provided in Attachment A to brief your colleagues.

### Recommendations

It is recommended that you:

- |    |   |          |
|----|---|----------|
| 1. | <b>Agree</b> to consult Ministerial colleagues on the enclosed draft Cabinet paper.   | YES / NO |
| 2. | Subject to Ministerial consultation, <b>agree</b> to lodge the paper by 26 March for consideration by the Cabinet Social Wellbeing Committee on 1 April 2020. | YES / NO |

 Tony Lynch Deputy Chief Executive, National Security Group
11/03/20 ...../...../.....

Hon Kris Faafoi Minister of Broadcasting, Communications and Digital Media
...../...../.....

~~IN CONFIDENCE~~

**Contact for telephone discussion if required:**

Name	Position	Telephone		1st contact
Sophie Vickers	Team Manager, National Security Policy Directorate	9(2)(a)	9(2)(a)	✓
6(a)	Senior Advisor, National Security Policy Directorate	9(2)(a)	9(2)(a)	

**Minister's office comments:**

- ☐ Noted
- ☐ Seen
- ☐ Approved
- ☐ Needs change
- ☐ Withdrawn
- ☐ Not seen by Minister
- ☐ Overtaken by events
- ☐ Referred to



# CABINET PAPER: IN-PRINCIPLE DECISION ON ACCESSION TO THE BUDAPEST CONVENTION

## Background

3. In October 2018 you agreed to take a joint paper to Cabinet – along with the Minister of Justice – seeking Cabinet's agreement for New Zealand to accede to the Budapest Convention. This paper noted that only minor amendments would be required to bring New Zealand laws into alignment with the Budapest Convention, of which the creation of a data preservation scheme is the most significant.
4. You and Hon Little instructed officials to draft a Cabinet paper and to consult with telecom companies about the details of a data preservation scheme. Consultation with telecom companies was carried out in March 2019, <sup>9(2)(ba)(i)</sup>
5. Last November, you agreed to delay the taking of the Cabinet paper until early 2020 to allow for targeted engagement with Māori. In January, officials met with representatives of Māori-owned tech firms, along with academics and other experts on Māori data sovereignty. This engagement was positive, surfacing a range of interests within the wider cyber policy domain. However, participants did not believe they had enough information about the Budapest Convention itself to confirm their interests in accession.
6. In February 2020, you agreed that officials follow a two-stage process for accession, with an in-principle decision to be taken by Cabinet in March/early April, alongside approval to engage formally with Māori and other interested parties on a draft National Interest Analysis document. This would inform a further Cabinet decision in June on accession.
7. Officials from the Department of the Prime Minister and Cabinet and Crown Law have subsequently prepared the attached Cabinet paper and consultation document, in consultation with the Ministry of Justice.

## The Cabinet paper proposes a two-step approach to accession

8. The attached paper proposes a two-step process to enable accession to the Budapest Convention: an in-principle decision to be taken by Cabinet in early April, to be followed by a further decision in June.
9. An in-principle decision in April would enable the Minister of Foreign Affairs to formally express New Zealand's interest in acceding. This would trigger the Council of Europe to issue New Zealand with an invitation to accede, which would give New Zealand "invited party" status for five years. During these five years, New Zealand would be able to participate in ongoing negotiations on additional protocols to the Convention, while completing all the necessary steps to accede (including parliamentary treaty examination and passage of required legislation).
10. This two-step approach (in-principle decision in April, to be followed by a further decision in June) balances our need to secure our international interests at a critical time alongside a

desire to engage further with Māori.<sup>1</sup> In particular, in terms of our pressing international interests:

- Parties to the Budapest Convention are set to negotiate a Second Additional Protocol to the Convention in 6(b). New Zealand must formally express an interest in accession by early April to participate 6(b). The Second Additional Protocol seeks to improve the efficiency of mutual assistance processes regarding access to electronic evidence held in the cloud. 9(2)(h)

- 6(a)  
New Zealand's expression of interest in joining the Budapest Convention at this time will send a strong signal of our support for the Convention and its protection of human rights and freedoms;

- 6(a), 6(b)

and

- 6(a), 9(2)(f)(iv)

11. The Ministry of Foreign Affairs and Trade has confirmed that expressing interest in accession would represent a political commitment to accede to the Budapest Convention, but that it would not be legally binding.
12. The standard process towards accession would be to seek Cabinet agreement in a single paper. However, given the desire to balance international interests with further engagement domestically, agencies support the proposed two-step approach to accession (including Crown Law, the Ministry of Justice, and the Ministry of Foreign Affairs and Trade).

### **Proposed next steps on consultation ahead of the June confirmation**

13. Advice from the Ministry of Foreign Affairs and Trade is that the National Interest Analysis (NIA) should not be publicly released at this stage. As the NIA is drafted for Parliament, the authority to publish rests with Parliament rather than Cabinet. Therefore, we have instead prepared a public consultation document for release that we can use for informal and formal consultation with stakeholders.
14. It is proposed that this consultation document be released for further public engagement (in particular, with Māori) ahead of the June Cabinet paper seeking a further decision on

<sup>1</sup> Participants in the hui in January explicitly requested that further opportunities be provided for a wider range of Māori groups to make their views known to the Crown.



accession. This engagement will feed into the National Interest Analysis that will accompany the June Cabinet paper, which would need to be submitted to Parliament for scrutiny.

15. Further engagement will ensure that officials are able to confidently advise Cabinet on Māori and other interests in the Convention and, if Cabinet agrees to proceed, whether New Zealand should make any formal declarations or reservations as part of acceding to the Budapest Convention.<sup>2</sup> Formal declarations provide a potential avenue for communicating to other parties to the Budapest Convention how New Zealand interprets various provisions of that Convention. 9(2)(f)(iv)
- [REDACTED]

## Consultation

---

16. The draft paper has been consulted with the following agencies: Crown Law; Customs; Department of Internal Affairs; Government Communications Security Bureau; Ministry of Business, Innovation and Employment; Ministry of Foreign Affairs and Trade; New Zealand Security Intelligence Service; New Zealand Police; Treasury; Te Arawhiti; and the State Services Commission.

17. 9(2)(h)
- [REDACTED]

## Financial Implications

---

18. 9(2)(f)(iv)
- [REDACTED]

19. There are no direct financial implications of the attached in-principle Cabinet paper. However, the paper does note that there will be implications associated with the second paper in June, 9(2)(f)(iv)
- [REDACTED]

20. The Ministry of Justice has advised that there are options available to progress with accession 9(2)(f)(iv). Upon receiving invited party status, New Zealand will have five years in which to progress all the necessary steps to accede. During this time:

- 9(2)(f)(iv)
- [REDACTED]

---

<sup>2</sup> As outlined in the Cabinet paper, the current proposal is that New Zealand join other common law countries that have acceded to the convention in making one reservation. This reservation relates to a clause in the convention providing for the creation of universal jurisdiction in relation to certain criminal offences.

## Next Steps

---

21. Subject to Cabinet approval, officials will provide the Minister of Foreign Affairs with a draft letter to send to the Council of Europe, and will release the consultation document for formal public consultation.
22. Following the public consultation process, a second Cabinet paper will be submitted in June 2020. This paper will include the full policy decisions on acceding to the Budapest Convention for Cabinet's consideration.

Attachments:	Classification:	
A:	IC	Speaking points for SWC
B:	R	Draft Cabinet Paper: Approval to initiate the first stage towards accession to the Budapest Convention



## ATTACHMENT A: SPEAKING POINTS

### Budapest Convention

- This paper seeks approval for New Zealand's accession to the Budapest Convention – an international treaty seeking specifically to address internet and computer crime.
- New Zealand has been looking to accede to this Convention since its inception in 2004 and it has been mentioned in the past three cyber security strategies as being a key deliverable to supporting our goals for a safer and more secure cyber environment.
- Cybercrime is increasing every year worldwide and New Zealand is not immune. This includes crimes committed via the internet and other computer networks, particularly infringements of copyright, computer-related fraud, child pornography and violations of network security. Cybercrime is complex to detect and prosecute because it is borderless.
- The Convention addresses cross-border cybercrime by aligning nations' laws, facilitating information-sharing on current threats and best practice, increasing international cooperation, and fostering international dialogue.
- I'm of the view that it is in New Zealand's best interests to participate in the only existing international treaty to tackle cybercrime.
- We already comply with most of the legislative and regulatory requirements and we would need only minor changes to our domestic legislation, which are outlined in the Cabinet paper.

### Benefits

- Accession to the Budapest Convention will have real benefits for the way in which we cooperate internationally to tackle cybercrime.
- It will also reputational benefits for New Zealand, and would signal that we are serious about cooperating with other countries in combating crime through reciprocal information-sharing.
- There are currently 64 member countries. New Zealand is the only Five Eyes partner that is not a member. This stands in contrast to our statements on this issue. For instance, in July 2019 Attorney-General Hon David Parker signed the Quintet of Attorneys General statement on international cooperation on cybercrime.<sup>6(a)</sup>

- 6(a), 6(b)

- 6(a), 6(b)

- 6(a), 6(b)

### Consultation

- This paper recommends we release a public consultation document on the Convention for interested stakeholders, primarily Māori and telecom companies.
- In January, officials met with representatives of Māori-owned tech firms, along with academics and other experts on Māori data sovereignty. This engagement was positive, identifying a range of Māori interests within the wider cyber policy domain. However, participants did not believe they had enough information about the Budapest Convention itself to confirm their interests in accession.
- The telecom companies were consulted on the data preservation scheme requirement of acceding to the Convention. 9(2)(ba)(i)

### Next Steps

- To initiate the process of accession, the Minister of Foreign Affairs would need to send a letter to the Council of Europe expressing interest in acceding to the Convention. The Council of Europe would then respond within 2-3 months with a formal invitation to become a member to the Convention. We would then have "invited party" status to the Convention, and would be able to attend meetings as an observer.
- There is a negotiation 6(b) on an additional Protocol to the Convention, which will include cooperation on law enforcement access to evidence held in the cloud, mutual assistance for electronic evidence, and safeguards around data protection.
- We think it is important New Zealand is at that meeting as these topics are of interest to us, 6(b)
- Although MFAT has confirmed that New Zealand expressing interest in accession would represent a political commitment to accede to the Budapest Convention, it would not be legally binding.
- We see this approach as enabling us to continue genuine engagement with Māori and other stakeholders to better inform a decision on accession, while ensuring we can have a voice in important negotiations on expanding the Convention.
- By being at the table during 6(b) negotiations, we will also be able to better identify any Māori interests in the issues being discussed.
- Following the public consultation process, a second Cabinet paper will be submitted in June 2020. This paper will include the full policy decisions on acceding to the Budapest Convention, for Cabinet's consideration.



## Accession to the Budapest Convention – Cabinet paper

Hon Andrew Little, Minister of Justice

12 March 2020

### Purpose

1. This aide memoire will support your discussion at SWC on 1 April about the attached Cabinet paper seeking an in-principle decision for New Zealand to accede to the Council of Europe's Budapest Convention on Cyber Crime ("the Budapest Convention").

### Background on the Budapest Convention and work to date

2. The Budapest Convention seeks to harmonise international laws on cybercrime. It enables international cooperation between law enforcement agencies and the sharing of best practice on countering cyber threats. The Budapest Convention establishes a model law that covers:
  - pure cybercrime – criminal acts where a computer or network is the target of the offence (e.g. deploying malicious software);
  - cyber-enabled crime – criminal acts that are assisted by technology (e.g. cyber-enabled fraud or the distribution of child exploitation material); and
  - law enforcement access to criminal evidence stored electronically.
3. In October 2018 you agreed to take a joint paper to Cabinet – along with Hon Faafoi, the Minister of Broadcasting, Communications and Digital Media – seeking Cabinet's agreement for New Zealand to accede to the Budapest Convention (DPC-2017/18-1337 refers). This paper noted that only minor amendments would be required to bring New Zealand laws into alignment with the Budapest Convention, of which the creation of a data preservation scheme is the most significant.
4. You and Hon Faafoi instructed officials to draft a Cabinet paper and to consult with telecom companies about the details of a data preservation scheme. Consultation with telecom companies was carried out in March 2019, <sup>9(2)(b)(ii)</sup>
5. Last November, Hon Faafoi agreed to delay the Cabinet paper until early 2020 to allow for targeted engagement with Māori. In January, officials met with representatives of Māori-owned tech firms, along with academics and other experts on Māori data sovereignty. This engagement was positive, surfacing a range of interests within the wider cyber policy domain. However, participants did not feel ready to confirm their specific interests in accession.

### The Cabinet paper proposes a two-step approach to accession

6. The attached paper proposes a two-step process to enable accession to the Budapest Convention – an in-principle decision to be taken by Cabinet in early April, to be followed by a confirmation decision in June.
7. An in-principle decision in April would enable the Minister of Foreign Affairs to formally express New Zealand's interest in acceding. This would trigger the Council of Europe to

<sup>1</sup> 17 telecommunication companies and Internet NZ were invited to provide comment on the creation of a data preservation scheme, eight provided comment.

issue New Zealand with an invitation to accede, which would give New Zealand “invited party” status for five years. During these five years, New Zealand would be able to participate in ongoing negotiations on additional protocols to the Convention, while completing all the necessary steps to accede (including parliamentary treaty examination and passage of required legislation).

8. This two-step approach balances our desire to engage further with Māori with the following pressing international interests:<sup>2</sup>

- parties to the Budapest Convention are set to negotiate a Second Additional Protocol to the Convention <sup>6(b)</sup> [redacted] New Zealand must express an interest in accession by early-Apr [redacted] pate. The Protocol seeks to regulate international law enforcement access to evidence held in the cloud. <sup>9(2)(h)</sup> [redacted]

- <sup>6(a), 6(b)</sup> [redacted]

- New Zealand is the only five-eyes member not party to the Budapest Convention. <sup>6(a), 6(b)</sup> [redacted]

- <sup>6(a), 9(2)(f)(iv)</sup> [redacted]

9. The Ministry of Foreign Affairs and Trade has confirmed that New Zealand expressing invitation to accede would represent a political commitment to accede to the Budapest Convention, but that it would not be legally binding.

#### **Proposed next steps on consultation ahead of the June confirmation**

10. A consultation document outlining the impact for New Zealand of accession to the Budapest Convention is attached to the Cabinet paper. It is proposed that this document be released for further public engagement ahead of the June Cabinet paper. This engagement will feed into the National Interest Analysis that will accompany the June Cabinet paper, which will need to be submitted to Parliament for scrutiny.
11. Further engagement will ensure that officials are able to confidently advise Cabinet on whether New Zealand should make any formal declarations or reservations as part of accession.<sup>3</sup> <sup>9(2)(f)(iv)</sup> [redacted]

<sup>2</sup> Participants in the hui in January explicitly requested that further opportunities be provided for a wider range of Māori groups to make their views known to the Crown.



9(2)(f)(iv)

### Interaction with Budget 2020

12. 9(2)(f)(iv)

13. There are no direct financial implications of the attached in-principle Cabinet paper. However, the paper does note that there will be implications associated with the confirmation paper in June 9(2)(f)(iv)

14. There are options available to progress with accession 9(2)(f)(iv)  
Upon receiving invited party status, New Zealand will have all the necessary steps to accede. During this time:

- 9(2)(f)(iv)
- 

Released under the Official Information Act 1982



## Accession to the Budapest Convention – Cabinet paper

Hon Andrew Little, Minister of Justice

20 May 2020

### Purpose

1. This note updates you on a Cabinet paper that you are jointly taking to the Social Wellbeing Committee on 27 May with Minister Faafoi. The paper seeks in-principle approval for New Zealand to accede to the Council of Europe's Budapest Convention on Cyber Crime ("the Budapest Convention"), and approval to further public consultation on the matter.


### Background on the Budapest Convention and work to date

2. In October 2018 you agreed to take a paper to Cabinet – with the Minister of Broadcasting, Communications and Digital Media – seeking Cabinet's agreement for New Zealand to accede to the Budapest Convention (DPC-2017/18-1337 refers). This paper noted that only minor amendments would be required to bring New Zealand laws into alignment with the Budapest Convention, of which the creation of a data preservation scheme is the most significant.<sup>1</sup> Minister Faafoi's office has led ministerial consultation on the paper.
3. The Budapest Convention seeks to harmonise international laws on cybercrime. It enables international cooperation between law enforcement agencies and the sharing of best practice on countering cyber threats. The Budapest Convention establishes a model law that covers:
  - pure cybercrime – criminal acts where a computer or network is the target of the offence (e.g. deploying malicious software);
  - cyber-enabled crime – criminal acts that are assisted by technology (e.g. cyber-enabled fraud or the distribution of child exploitation material); and
  - law enforcement access to criminal evidence stored electronically.
4. You and Minister Faafoi previously instructed officials to consult with telecom companies about the details of a data preservation scheme. Consultation with telecom companies was carried out in March 2019, <sup>9(2)(b)(ii)</sup>
5. Last November, Hon Faafoi agreed to delay the taking of the Cabinet paper until early 2020 to allow for targeted engagement with Māori. In January, officials met with representatives of Māori-owned tech firms, along with academics and other experts on Māori data sovereignty. This engagement was positive, surfacing a range of interests within the wider cyber policy domain. However, participants did not believe they had sufficiently engaged with the Budapest Convention itself to confirm their interests in accession.


<sup>1</sup> A data preservation scheme would enable orders to be issued requiring technology companies to temporarily refrain from deleting information related to criminal offending. This allows time for mutual assistance requests from foreign jurisdictions to be processed by Crown Law and production orders to be sought under the Search and Surveillance Act, if appropriate.

<sup>2</sup> 17 telecommunication companies and Internet NZ were invited to provide comment on the creation of a data preservation scheme, eight provided comment.

## **This paper is the first step towards accession, but further work is required**

6. The attached paper proposes a three-step process to enable accession to the Budapest Convention – an in-principle decision to be taken now, to be followed by public consultation later this year, and a confirmatory decision in April 2021.
7. The first step is an in-principle decision from Cabinet. This will enable New Zealand to gain “invited party” status for five years and will allow us to take part in negotiations (occurring later this year) on a potential Second Additional Protocol to the Convention. This Additional Protocol relates to international law enforcement cooperation and mutual assistance in respect of criminal evidence held in “the cloud”. <sup>9(2)(h)</sup>  

8. The second step is to consult further with the public on the proposal. The paper seeks Cabinet's agreement to publish the consultation document in annex one. This will support further engagement (later in the year) with the telecommunications industry, Māori, and civil society (particularly groups with an interest in human rights and privacy). Consultation with these groups to date have been positive, but parties have indicated that further detailed information about the convention is required to support them to identify their full range of interests.<sup>3</sup>
9. The third step is to come back to Cabinet in April 2021 seeking a final decision on accession. This paper will include detail on the legislative changes required to progress accession, taking into account information gained from consultation, and will include a full national interest analysis. This would trigger Parliamentary Treaty Examination before legislation was introduced.

## **Implications for future Budget rounds**

10. There are no costs to the Crown arising from this paper. However, if Cabinet does confirm its decision to accede next year there could be some financial implications, specifically:
  - a) Costs incurred by telecommunications and other companies in complying with data preservation orders. These costs are estimated at approximately \$1.5 million per annum. However, this figure is sensitive to the design of the scheme, including the scope of preservation orders, and the scale of requests under the Convention. A decision would be required about whether the Crown would contribute to those costs, and if so, the model for cost allocation.
  - b) Operational departmental costs to progress and implement the legislative changes required to accede, and to service New Zealand's participation in the Convention (including travel costs and overheads).
11. Further advice on the financial implications will be provided when officials report back to Cabinet in April 2021. <sup>9(2)(f)(iv)</sup>  


<sup>3</sup> Participants in the hui in January explicitly requested that further opportunities be provided for a wider range of Māori groups to make their views known to the Crown.



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

# Aide-Memoire

## SOCIAL WELLBEING COMMITTEE DISCUSSION ON ACCESSION TO THE BUDAPEST CONVENTION ON CYBERCRIME: SPEAKING POINTS

To Hon Kris Faafoi, Minister for Broadcasting, Communications, and Digital Media

Date	22/05/2020	Priority	Routine
Deadline	26/05/2020	Briefing Number	1920NSP/075

### Purpose

The Cabinet paper seeking agreement in principle to accede to the Budapest Convention on Cybercrime has been lodged for discussion at Social Wellbeing Committee (SWC) on 27 May 2020. This aide-memoire provides suggested speaking points and background information for the discussion.

### Recommendations

1. **Note** the suggested speaking points and background information. YES / NO
2. **Agree** to forward this brief to the Minister of Justice. YES / NO

6(a)

Sophie Vickers  
Team Manager, National Cyber Policy  
Office, Department of the Prime  
Minister and Cabinet

22.../2020

Hon Kris Faafoi  
Minister of Broadcasting,  
Communications, and Digital Media

...../2020



**RESTRICTED**

**Contact for telephone discussion if required:**

Name	Position	Telephone		1st contact
Sophie Vickers	Team Manager, National Cyber Policy Office	9(2)(a)	9(2)(a)	✓
6(a)	Principal Policy Advisor, National Cyber Policy Office		9(2)(a)	

**Minister's office comments:**

- ☐ Noted
- ☐ Seen
- ☐ Approved
- ☐ Needs change
- ☐ Withdrawn
- ☐ Not seen by Minister
- ☐ Overtaken by events
- ☐ Referred to

## BUDAPEST CONVENTION: SPEAKING POINTS FOR SWC

### Summary

- This paper seeks approval in principle for New Zealand's accession to the Budapest Convention – an international treaty seeking to address internet and computer crime.
- The Convention was drafted by the Council of Europe, but is open for accession by any country, and now has 65 members.
- We would be acceding in good company: 6(a)
- Joining is consistent with the Cyber Security Strategy and the countering violent extremism work programme.
- Our legislation is largely aligned with the Convention; only incremental changes would be required.
- The proposed approach allows for extensive consultation on the implications of joining, and final decisions by Cabinet in April next year.

### FURTHER INFORMATION IF REQUIRED

- New Zealand has been looking to accede to this Convention for over ten years. It supports our goals for a safer and more secure cyber environment.
- Cybercrime is increasing every year. This includes crimes committed via the internet and other computer networks, such as infringements of copyright, computer-related fraud, violations of network security, spreading violent extremist content and child pornography.
- Cybercrime is hard to detect and prosecute because it is borderless. COVID-19 has highlighted the need for strong international collaboration on cybercrime: the crisis has been rapidly exploited by cybercriminals across the globe.
- The Convention addresses cross-border cybercrime by aligning nations' laws, facilitating information-sharing on current threats and best practice, increasing international cooperation, and fostering international dialogue.

### Accession complements New Zealand's existing and strong cooperation on cybercrime, without fundamental changes to how we work with others

- Accession would enhance our access to information for criminal investigations, as well as information on best practice for cybercrime investigations and threat trends.
- It would strengthen the relationships we have with member countries, and help us build relationships with countries with whom we do not have existing partnerships. We would have access to a 24/7 network of contacts for assistance from member countries.
- The legal changes required would complement existing mutual assistance laws.
- Accession would allow us to become a member of the Cybercrime Convention Committee, contributing to global dialogue on this global problem, including participating in negotiations on extensions to the Convention.

RESTRICTED

**Accession would signal that we are serious about working with others to combat cybercrime**

- There are currently 65 member countries. 6(a)  
[REDACTED]
- It also stands in contrast with our statements on this issue: 6(a)  
[REDACTED] the Attorney General has publicly confirmed support for the Convention, along with his Five Eyes counterparts.

6(a)

- 6(a), 6(b)  
[REDACTED]

- 6(a)  
[REDACTED]

**There would be a three stage process towards accession**

- **An in-principle decision to accede.** This would allow the Minister of Foreign Affairs to write to the Council of Europe expressing interest in accession. If the Council of Europe responds favourably, officials would be able to attend convention meetings as observers.
- This is important because there are negotiations 6(b) on an expansion to the Convention that will shape future global cybercrime law and practice.
- **A consultation on the impacts of accession.** A consultation document would be published later this year. Targeted engagement would take place alongside that, with the telecommunications industry, with Māori and with civil society.
- Telecommunications firms have already been consulted on the implications of a data preservation scheme – one of the Convention's requirements. 9(2)(ba)(i)  
[REDACTED] Officials will engage further with firms on the design of a scheme, and the costs, and then provide advice on how costs might be allocated.
- An initial hui was held to discuss Māori interests in the Convention. The hui confirmed that it does touch on areas of Māori interest, and that we need to more clearly explain and discuss the implications of joining in order for Māori to give a view. More engagement is appropriate before a final decision. The hui demonstrated interest in wider discussion on cyber policy.
- An incremental expansion of mutual assistance powers would be required, and a new power added to the Search and Surveillance Act. Consultation will allow us to explore the changes with civil society, and demonstrate the safeguards that ensure our collaboration on cybercrime is in line with our human rights and privacy frameworks.
- The Privacy Commissioner has been consulted and is supportive. The Convention supports and upholds the right to privacy and the importance of data protection.
- **A final Cabinet paper in April 2021.** Cabinet would take a final decision on whether to proceed with accession, and how to implement it in law, taking into account information gained from consultation. Parliamentary Treaty Examination and legislation would follow.



9(2)(g)(i)

Released under the Official Information Act 1982



## EXAMPLES OF HOW THE LEGAL CHANGES REQUIRED FOR ACCESSION COULD ENHANCE ACCESS TO DATA FOR CRIMINAL INVESTIGATIONS

### Adding data preservation orders to the Search and Surveillance Act

- Example: The police could, on behalf of a foreign counterpart, require a telecommunications company to temporarily hold on to recently stored information about a suspect's location, the timing of phone conversations and the parties to those conversations, for use in an overseas criminal investigation. The foreign counterpart would then make an application for mutual legal assistance, in the knowledge that the relevant data had been preserved. The application would be reviewed by Crown Law and, if approved, legal authority would be granted to obtain the information. Likewise, New Zealand would be able to request that a foreign counterpart use their parallel powers to preserve information in support of a New Zealand criminal investigation.
- Outcome: There would be less risk that data relevant to the investigation would be destroyed before the 6-18 month mutual legal assistance process is complete.
- Note: Domestically, NZ Police uses production orders under the Search and Surveillance Act to obtain telecommunications information. However, preservation orders may be used in future for domestic investigations in certain circumstances.

### Adding surveillance device warrants to the Mutual Assistance in Criminal Matters Act

- Example: A partner country could request that New Zealand Police use a surveillance device warrant to conduct audio surveillance of communications of a member of a child sexual exploitation network operating across multiple countries. Such warrants can only be used for crimes punishable by imprisonment for 7 years or more. If approved, the evidence obtained would be shared via each country's central authority for mutual assistance, and could be used as evidence for an overseas prosecution. Likewise, New Zealand would be able to request that a foreign counterpart use their parallel powers to secure evidence for a New Zealand investigation or prosecution.
- Outcome: the evidence obtained may contribute to a more successful prosecution and reduce cross-border criminal offending.

### Introduce third party confidentiality orders to the Search and Surveillance Act

- Example: The police, when issuing a preservation order or surveillance device warrant to obtain evidence of a serious hack of a computer network, could require the internet service provider to keep the existence of the order or warrant confidential, if the investigation would be jeopardised by disclosure of the order.
- Outcome: The investigation would be more likely to proceed to court without being jeopardised by the premature awareness of the alleged offender that they were under investigation for a serious crime.
- Note: Third party confidentiality orders could be used to support both domestic and overseas investigations.



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

# Briefing

## BUDAPEST CONVENTION: TIMELINE FOR ENGAGEMENT AND FINAL DECISIONS ON ACCESSION

To: Minister of Broadcasting, Communications and Digital Media (Hon Kris Faafoi)

Date	28/05/2020	Priority	Urgent
Deadline	28/05/2020	Briefing Number	1920NSP/077

### Purpose

On 27 May 2020, Cabinet Social Wellbeing Committee considered a paper seeking approval in principle to accede to the Budapest Convention on Cybercrime, with final decisions to be taken by Cabinet in April 2021, informed by a period of consultation. The Committee invited you to consider how the timeline for taking final decisions on accession could be shortened, whilst ensuring sufficient time for engagement with Māori on matters that have been raised in initial consultation.

### Recommendations

1. **Note** that officials consider it would be possible to prepare a second paper on accession to the Budapest Convention for Cabinet consideration by the end of 2020;
2. **Note** that meeting that timetable would require public consultation and targeted engagement over the pre-election period;
3. **Note** that iwi, Māori organisations and wider stakeholders are under competing pressures as a result of the impacts of COVID-19, and this may limit their ability to engage with government on policy matters;
4. **Agree** to amend the draft Cabinet paper to seek Cabinet agreement for a second paper to be submitted to Cabinet by the end of 2020; and

YES/NO

BUDAPEST CONVENTION: TIMELINE FOR ENGAGEMENT AND FINAL DECISIONS ON ACCESSION

Report No.

5. If you agree, **refer** this paper to the Ministers of Justice and Māori Crown Relations: Te Arawhiti.

YES/NO

 Tony Lynch <b>Deputy Chief Executive National Security Group Department of the Prime Minister and Cabinet</b>
28.05.20 ...../...../.....

  Hon Kris Faafoi <b>Minister for Broadcasting, Communications and Digital Media</b>
...../...../.....



# BUDAPEST CONVENTION: TIMELINE FOR ENGAGEMENT AND FINAL DECISIONS ON ACCESSION

## Potential timeline for engagement and final decisions

1. The paper considered by the Social Wellbeing Committee on 27 May 2020 proposed that Cabinet would take final policy decisions on accession in April 2021, after a public consultation process later this year. This timeline allowed for an extended period of engagement, including a public written consultation and targeted consultation with Māori, civil society and the telecommunications industry.
2. An alternative timeline could be met for final policy decisions on accession by the end of the year, if:
  - a) consultation and engagement takes place during the pre-election period, with a written consultation period of eight weeks;
  - b) Māori groups and other partners that we have identified as potential engagement partners are able and willing to prioritise engagement on this topic, amongst a range of competing demands and pressures arising from COVID-19;
  - c) agencies prioritise policy and communications resource to support the consultation, submissions analysis and policy development process; and
  - d) we are able to get agency and, where necessary, Ministerial, agreement to materials needed to support consultation in good time, including on an indicative proposal for a data preservation scheme.
3. These issues are outlined in more detail below. An indicative timeline aiming for submission of the second Cabinet paper in October 2020 is attached at Annex A.

## Engagement and consultation during the pre-election period

4. For Cabinet to take final decisions by the end of the year, it will be necessary for agencies to consult and engage during the pre-election period. Cabinet Office Circular CO (20) 1 provides guidance on government decisions and actions during the pre-election period. There are no specific conventions on consultation during a pre-election period and the government continues to have full power to make decisions during that period.
5. Cabinet Office has provided guidance, stating that the consultation for the Budapest Convention accession is business-as-usual activity that can proceed in the pre-election period, so long as consultation material is consistent with the Government Advertising Guidelines. In particular, that any documentation and supporting information should be presented in an objective and transparent manner to avoid any risk that it might be perceived that funds are being used to finance publicity for party political purposes.



## Potential partners for Māori engagement

6. Following the hui in January, we have identified four potential groups for Māori engagement, whose areas of interest align with the subject matter of the Budapest Convention:
- Te Hunga Rōia Māori (the Māori Law Society)
  - Te Mana Raraunga (Māori Data Sovereignty Network)
  - Data Iwi Leaders Group
  - NZ Māori Council
7. Engagement had planned to take the form of a series of hui to explore the implications, benefits, costs and risks of accession in more detail, in the context of the existing legal framework for search and surveillance and mutual legal assistance. <sup>9(2)(f)(iv)</sup>
8. The hui will be most effective if they can take place as face-to-face meetings. Like the hui in January, budget can be provided to facilitate iwi traveling to Wellington. However, COVID-19 may prevent some travel. Te Arawhiti has advised that, as an alternative, engagement could take place via:
- Small face to face meetings;
  - Virtual meetings through Zoom; and
  - Phone calls with stakeholders.
9. Iwi efforts are currently focussed on protecting and supporting their communities through the impacts of COVID-19, and their capacity to concentrate on other issues may be limited. Once Cabinet has taken a decision, and an announcement made, we will initiate contact with potential partners to understand their willingness and capacity to consider these matters in July and August.
10. Our recommendation is that we assess in September whether sufficient progress has been made in this engagement to be able to meet the proposed timeline for final decisions.

## Partners for wider engagement

11. Engagement with the telecommunications industry and other technology companies is needed on the policy design of a proposed data preservation scheme, in order to make recommendations to Cabinet on the design of the scheme, its costs, and how costs might be allocated. The telecommunications sector is currently facing pressure as a result of COVID-19 and wider matters.
12. Feedback from the prior consultation in 2019 included a request for more detail on how data preservation orders would affect them. To make it as easy as possible for industry to engage, we propose engaging with telecommunications companies early, providing them

with a draft of the scheme including examples of preservation orders, and estimates of how many preservation and production orders can be expected domestically and internationally.

13. The most significant impact on resourcing will be to complete the design of a data preservation scheme with sufficient detail to enable useful consultation with the telecommunication companies. Material for this consultation will need to be prepared by June.
14. Engagement with civil society organisations will be an opportunity to introduce the proposed legislative changes required by Budapest accession and discuss any concerns that might come up. A small number of workshops would likely be a good way to manage this, to support organisations in their written responses to the consultation.

### **Agency resourcing constraints**

---

15. DPMC will seek assistance from other agencies to meet the shortened timeframe. This will require prioritisation across a number of agencies to support this work.

### **Consultation**

---

16. This briefing has been developed with consultation with Te Arawhiti, the Ministry of Justice, MBIE, Crown Law, NZ Police, and DIA.

### **Next Steps**

---

17. We have updated the Cabinet paper to bring forward the timeline for report back to late 2020, <sup>6(b)</sup> [REDACTED] and updated the financial recommendations. We will confirm the text of the financial recommendations after further consultation with the Ministry of Justice and Treasury on Friday morning.
18. If you agree with the proposed timeline, and subject to confirmation of the financial recommendation, we recommend you lodge the attached revised paper for Cabinet consideration.

# ANNEX A

## Potential timeline for engagement and Cabinet paper preparation by October 2020

	Main activities	Notes
June	<ul style="list-style-type: none"> <li>Announce intention to consult</li> <li>Talk to partners to work up consultation approach</li> <li>Finalise preparation for consultation</li> <li>Open written consultation (8 weeks)</li> <li>Begin Māori engagement</li> </ul>	Any further materials required to support consultation may require Ministerial approval
July		There will be four strands: public/written, Māori, civil society, telecommunications sector. The strands may have staggered start and end points
August	<ul style="list-style-type: none"> <li>Close written consultation</li> <li>Analysis of consultation responses</li> </ul>	
September	<ul style="list-style-type: none"> <li>Policy work on matters arising from consultation</li> <li>Update National Interest Analysis</li> <li>Update to Ministers on progress with Māori engagement and implications for timeline</li> </ul>	
October	<ul style="list-style-type: none"> <li>Advice and decisions on outcomes from consultation</li> <li>Review of National Interest Analysis</li> <li>Draft Cabinet paper</li> <li>Ministerial and Party consultation on Cabinet paper</li> <li>Cabinet final decisions</li> </ul>	
November	<ul style="list-style-type: none"> <li>9(2)(f)(iv)</li> </ul>	