MINISTRY OF JUSTICE
Tāhū o te Ture

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

Consultation paper:

New Zealand accession to the Budapest Convention on Cybercrime

New Zealand Government

July 2020

ISBN 978-0-947520-27-4

Contents

CONSULTATION PAPER: NEW ZEALAND ACCESSION TO THE BUDAPEST CONVENTION ON CYBERCRIME

1 The Department of the Prime Minister and Cabinet and Ministry of Justice are inviting public feedback on a proposal to join the Council of Europe Convention on Cybercrime (the Budapest Convention).

2 The Budapest Convention is an international treaty on internet and computer crime. It provides an international framework to address cybercrime and criminal evidence stored electronically.

3 New Zealanders are increasingly impacted by cybercrime, and offenders are increasingly using the internet and connected devices to commit or plan criminal activity.

4 New Zealand has already asked for an invitation to join the Budapest Convention as the first step in the process. This allows us access to support and information from the Council of Europe.

5 To ensure the Government can make an informed decision on joining the Budapest Convention, we want to hear from Māori, internet stakeholders, and the wider community, to better understand what impact New Zealand joining the Convention might have on you.

Submissions are public information

6 Note any submission you make becomes public information. People can ask for copies of submissions under the Official Information Act 1982 (OIA). The OIA says we have to make submissions available unless we have good reasons for withholding them. This is explained in sections 6 and 9 of the OIA.

7 Tell us if you think there are grounds to withhold specific information in your submission. The reasons for this might include that it is commercially sensitive, or that it's personal information. Any decision to withhold information can be reviewed by the Ombudsman, who may tell us to release it.

Use of information

8 The information provided in submissions will be used to inform analysis by the Department of the Prime Minister and Cabinet and the Ministry of Justice of the implications of New Zealand joining the Budapest Convention on Cybercrime, and to inform advice to Ministers. Submissions will be shared with other government agencies where necessary to facilitate analysis and development of advice. Material summarising the submissions received will be published as part of further documents relating to the Government's consideration of joining the Budapest Convention on Cybercrime.

9 Under the Privacy Act 1993, people have access to information held by agencies about them. Any personal information you send with your submission will only be used in relation to matters covered by this document. In your submission, please indicate if you prefer we do not include your name in any published summary of submissions.

Disclaimer

10 While every effort has been made to ensure the information in this publication is accurate, the Department of the Prime Minister and Cabinet and the Ministry of Justice do not accept any responsibility or liability for error of fact, omission, interpretation or opinion that may be present, nor for the consequences of any decisions based on this information.

What is the Budapest Convention?

11 The Budapest Convention is an international treaty that aims to prevent, deter and detect crimes committed via the internet and other computer networks, particularly infringements of copyright, computer-related fraud, child pornography and violations of network security, by enabling member countries to work together to combat cybercrime.

12 It does so by aligning nations' laws, facilitating information-sharing on current threats and best practice, increasing international cooperation, and fostering international dialogue.

13 The Budapest Convention came into force in 2004. There are currently 65 members of the Convention, predominantly from Europe, but also from Asia, North and South America, and the Pacific.

14 The Budapest Convention is a cybercrime convention in name, but its benefits extend more widely. It addresses:

a) pure cybercrime: a criminal act committed through the use of information and communication technologies or the internet, 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. An example of pure cybercrime is deploying malicious software;

b) cyber-enabled crime: any criminal act that could be committed without technology or the internet, but is assisted, facilitated or escalated in scale by the use of technology. This includes a range of serious and organised crime, such as cyber-enabled fraud, the distribution of child exploitation material, and terrorism;

c) criminal evidence stored electronically: for example, private social media communications relating to a crime, which are stored in the cloud by companies such as Facebook.

Why is New Zealand considering accession to the Budapest Convention?

Criminals are increasingly using the online environment

15 The Ministry of Justice's Crime and Victim Safety Survey published information in 2019 on cybercrime and financial crime. The results show that almost 400,000 people (about 7.5 percent of adults) experienced one or more incidents of fraud or cybercrime over the last 12 months. More than 200,000 adults were victims of one or more fraud incidents and more than 100,000 were victims of one or more cybercrime incidents. This compares to 355,000 households (20 percent of households) that experienced one or more property crime incidents over the last 12 months. The report noted that

fraud/deception and cybercrime are the offences least commonly reported to the Police (7 percent).

16 Cybercrime can include fraud, phishing scams, harassment, child exploitation material, terrorist content, identity theft and the illicit gaining of personal information for malicious purposes.

17 The online environment is attractive to offenders: it offers mass reach in respect of victims, with offending being conducted effortlessly across borders. Offenders also engage with each other using online technology that gives them anonymity.

18 Cybercrime can result in financial losses,[1] physical and mental harm as well as reputational damage. It can be frightening for victims and can prevent them from participating online, affecting their productivity, connectedness and quality of life.

19 Cybercrime is difficult to detect due to the high rate of offending, easy anonymity, avoidance of leaving traces of evidence of crimes, and the speed at which crimes can be committed and at which offenders can change tactics. Comparatively, the agency response takes a long time, has less resource and evidence of crime is dispersed across many jurisdictions.

20 Perpetrators of crimes against New Zealanders may use the online environment wholly or in part to commit crimes. Evidence of very serious crimes, including homicides, serious assaults, sexual assaults, frauds, and child exploitation is often found in online exchanges between victims and offenders.

Developing international partnerships to combat cybercrime

21 New Zealand agencies rely on international co-operation to prevent, mitigate, investigate and prosecute crimes committed wholly or in part online. This is simpler when all countries have consistent laws regarding how crimes committed online are defined and how agencies are able to access and use recorded evidence of crime.

22 Current information exchange and co-operation between different countries, for example through mutual legal assistance processes, is frequently slow and cumbersome, even where strong relationships exist.

23 Accession to the Budapest Convention would allow us to initiate or strengthen relationships with member countries by signalling our commitment to multilateral efforts to combat cybercrime. In addition, accession provides the opportunity to foster connections with member countries with whom do not have existing relationships. By providing a standardised framework for cooperation through aligned national cybercrime laws, the Convention makes it easier for countries to cooperate on criminal investigations of cybercrime and wider crimes involving electronic evidence.

[1] In 2019, 4741 cyber security incidents were reported to CERT NZ resulting in over $16.7 million in losses. The National Cyber Security Centre has calculated the value of harm directly prevented in 2018-19 was in excess of $27.7 million.

24 Accession would also demonstrate support for the best practice standards established by the Convention, and broader support for a rules-based international order. While the Convention sets out basic policies, it is up to each country to determine for themselves how to implement theses to enable an effective response in the context of their own constitutional arrangements, privacy settings, and security policies.

Alignment with cyber security policy objectives

25 New Zealand would benefit from membership of the Budapest Convention in order to deliver its strategic vision "New Zealand is confident and secure in the digital world: Enabling New Zealand to thrive online," as part of the Cyber Security Strategy 2019.[2] The strategy has five priorities to improve cyber security including to proactively tackle cybercrime.[3]

26 The National Plan to Address Cybercrime 2015 includes four priority actions:

1 - Build capacity to address cybercrime.

2 - Adapt New Zealand's policy and legislative settings to the digital age.

3 - Enhance New Zealand's operational response to cybercrime.

4 - Use New Zealand's international connections to combat cybercrime.[4]

27 The National Plan identifies exploring accession to the Budapest Convention as an important step in achieving these priorities.

Alignment with Government priorities

28 The Government has established 12 priority work streams.[5] Three of these priorities would be enhanced by New Zealand acceding to the Convention:

a) Support healthier, safer, and more connected communities

- Most New Zealanders depend on the internet for daily life, work or business. In order to keep communities healthier, safer and more connected, we need to detect, prevent, and investigate various forms of cybercrime to keep people safe online. The Convention would assist us by aligning New Zealand's cybercrime laws with international best practice, as well as streamlining the process for easier flow of information between member countries.

b) Make New Zealand the best place in the world for children

[2] New Zealand's Cyber Security Strategy 2019, Department of the Prime Minister and Cabinet, July 2019, p.8.
[3] The Strategy was refreshed following a Cabinet directive from 2018 that stated that it was timely to undertake a comprehensive refresh of New Zealand's cyber security settings to ensure that the government is investing the right resources in the right way across government to respond to growing cyber security threats.
[4] For the avoidance of doubt: while the current National Plan to Address Cybercrime was made under a previous Cyber Security Strategy, it remains in effect.
[5] The Government's priorities were established through developing 12 priority outcomes under three key themes as agreed to by Cabinet on 26 March 2018 [CAB-18-MIN-0111].

- It is vital we keep New Zealand children safe from exposure to, and becoming victims of, all cybercrimes. Children can be particularly vulnerable to the harms of child sexual exploitation material (CSEM) online. The Convention requires members to implement data preservation orders, which will further enhance the abilities of Customs and other agencies, including the Department of Internal Affairs and Police to detect, prevent and investigate child sexual exploitation content, making New Zealand a safer place for children. Although New Zealand does not have to be a member of the Convention to pass data preservation laws, accession provides a good opportunity to enable this change along with the other suite of changes that are a requirement of the Convention.

c) Create an international reputation we can be proud of

- Accession would demonstrate New Zealand's support for the best practice standards established by the Convention, and broader support for a rules-based international order.

Law Commission recommendations

29 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.[6] The resulting report recommended that the Government consider accession to the Budapest Convention.

30 The Law Commission also undertook extensive consultation as part of its review of mutual assistance and extradition law, including consideration of including surveillance device warrants in the mutual assistance scheme. In February 2016 the Law Commission issued its report: Modernising New Zealand's Extradition and Mutual Assistance Laws.[7] One of the main principles of the Law Commission report is that powers that are available to domestic authorities should be available in response to requests for assistance in foreign criminal matters.

[6] Law Commission and Ministry of Justice *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

[7] Law Commission *Modernising New Zealand's Extradition and Mutual Assistance Laws http://r137.publications.lawcom.govt.nz/*

Legal obligations imposed on New Zealand by accession to the Budapest Convention

31 If New Zealand decided to accede to the Budapest Convention, it would need to adhere to a range of procedural provisions on cybercrime, to enable better international co-operation in investigating cybercrime and obtaining electronic evidence for all types of crime. Some of these are to be incorporated in New Zealand legislation and some would apply only at the Convention level.

32 These provisions include that:

- procedural powers for the investigation of cybercrime should be established, implemented, and applied in a way that adequately protects human rights (Article 15);
- cybercrime offences the Convention applies to shall be deemed to be extraditable offences between Convention parties (Article 24);
- convention parties shall "afford one another mutual assistance to the widest extent possible" for investigating cybercrime offences or the collection of electronic evidence (Article 25);
- states must implement procedural requirements for mutual assistance requests, including designating a central authority; and the requesting and requested parties' ability to request confidentiality for mutual assistance information; (Articles 27 & 28);
- stateparties are able to request that other parties preserve data in respect of which the requesting party intends to submit a request for mutual assistance (Articles 29 & 30);
- parties would provide mutual assistance to one another (according to their domestic laws) regarding access to data, and do so on an expedited basis where there are grounds to believe that relevant data is vulnerable to loss or modification (Article 31);
- states party may access or receive computer data located in the territories of other states party, if they obtain the consent of the person who has the lawful authority to disclose that data (Article 32).

33 Implementing legislation would be required to bring New Zealand law in line with these provisions. Most of the required tools are already in place domestically, but there are some gaps. Changes 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, would be required. They would cover:

- data preservation orders (which would require entities that hold specific information relevant to a specific criminal investigation to preserve that information temporarily on their systems, while a production order is sought);

- 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);
- adjustments to New Zealand's mutual assistance law, in particular extending the availability of surveillance device warrants from the Search and Surveillance Act to the Mutual Assistance in Criminal Matters Act, so they could be used in New Zealand to obtain information relevant to overseas investigations, and vice versa;
- minor changes to some elements of our computer crime offences;
- an Order in Council prohibiting the import of a physical device for a computer crime.

34 More detailed information on these changes is set out in Appendix A.

Dispute settlement mechanisms

35 Per article 45 of the Budapest Convention, state parties would seek to settle any dispute between themselves through negotiation managed by the European Committee on Crime Problems.

Reservations to the Budapest Convention

36 Parties can enter reservations for specific provisions of the Budapest Convention per Article 42.

37 Officials are exploring whether to recommend invoking one reservation to the Convention, to Article 22(1)(d). This article requires parties to establish jurisdiction over their citizens if they commit a Convention offence, regardless of where the crime was committed. Section 7A of the Crimes Act 1961 currently extends extraterritoriality in some circumstances to New Zealand citizens who commit a crime outside of the country. However, this is reserved only for serious offences in the Crimes Act with a penalty or seven or more years' imprisonment, or offences under the Terrorism Suppression Act 2002. Argentina, Australia, Belgium, Canada, Chile, France, Israel, Japan, Turkey, the UK and the US have reservations to this article. Officials will explore further whether New Zealand should take a similar approach, noting our existing provisions for extraterritorial jurisdiction.

Advantages, implications and costs of New Zealand acceding to the Budapest Convention

Advantages

38 Accession would allow agencies to respond more effectively to cybercrime, especially cross-border cybercrime (including transnational organised cybercrime) and crime following international trends (as there would be better threat intelligence from accession).[8] Advantages of accession to the Budapest Convention include the following:

a) The Budapest Convention makes general and specific provisions for cooperation among Parties "to the widest extent possible" not only with respect to cybercrime, but more widely with respect to any crime involving electronic evidence. New Zealand's accession to the Budapest Convention would enhance and complement New Zealand's existing access to investigative data that can be used as evidence in criminal cases, intelligence on malicious actors, investigatory best practices, and threat trends.

b) The Budapest Convention provides a legal framework for international cooperation on cybercrime and electronic evidence. The Budapest Convention also includes provisions explicitly requiring that enforcement powers and procedures established under the Budapest Convention are to be conducted with respect for fundamental human rights and liberties, such as freedom of expression and protection of privacy and personal data.[9]

c) Parties to the Budapest Convention engage with each other in trusted and efficient cooperation. Currently, 65 states are parties and a number are in the process of accession. Membership may encourage expedited cooperation from other member countries, particularly countries with which New Zealand does not have a separate bilateral agreement. Additionally it would give New Zealand access to and participation in the Budapest Convention's 24 hours a day/7 days a week network of contacts for the provision of assistance on an expedited basis.

d) The Council of Europe advises, from the experience so far, private sector entities are more likely to cooperate with criminal justice authorities of Parties to the Budapest Convention, as it provides evidence that Parties have a domestic legal framework on cybercrime and electronic evidence in place, including the necessary human rights safeguards.

e) The legislative amendments required for New Zealand to accede will complement existing mutual assistance laws, boosting capacity for international cooperation to deal with increasingly sophisticated and diverse forms of computer-related criminal activity. The amendments would include the ability to:

[8] See for example from Canada: Clough, *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, (2014) 40(3) Monash University Law Review 698-736: "the Convention provides the ideal vehicle for analysis of some of the specific challenges of achieving harmonisation."

[9] Article 15 – Conditions and Safeguards.

- require, for example, a social media company to preserve data for investigations (on request, for specific investigations);
- obtain a surveillance device warrant in New Zealand to access material relevant to overseas investigations, and vice versa, which is not currently possible under our mutual assistance legislation;
- require third parties such as internet service providers to keep the existence of a preservation order or surveillance device warrant confidential, if the investigation would be jeopardised by disclosure of the order.

f) New Zealand would become a member of the Cybercrime Convention Committee (T-CY), which is a comprehensive intergovernmental body dealing with cybercrime. Parties share information on cybercrime threat trends, best practice tips and experience, assess implementation of the Convention, and interpret the Convention through guidance notes.

g) New Zealand would also be able to participate in the negotiation of any future additional Protocols to the treaty, thus contributing to further evolution of the Budapest Convention and international rules and norms for combating cybercrime.

Human rights implications

39 Some legislative changes required for accession need to be considered in relation to the right to be free from unreasonable search and seizure. For example, extending mutual assistance means that other countries would be able to access a slightly expanded range of evidence collected in New Zealand.

40 We do not consider that the amendments to New Zealand law required by the Convention would provide for unreasonable search or seizure powers. 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, 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.

41 There are general provisions on human rights in the Budapest Convention, to which all states party must adhere. These cover due process, territorial sovereignty, and requiring human rights protections of state parties, and are broadly echoed in New Zealand law.

42 Further human rights considerations would also be undertaken as a part of making legislative changes:

a) The Ministry of Justice would undertake a human rights consideration process as part of the construction of any new offences or additional law enforcement powers.

b) The Crown Law Office would undertake further analysis of proposed legislative changes to ensure their consistency with the New Zealand Bill of Rights Act.

c) The Department of the Prime Minister and Cabinet and Ministry of Justice will work with the Privacy Commissioner to ensure the provisions of the Budapest Convention are enacted appropriately with respect to New Zealand's privacy framework. The Privacy Commissioner is supportive of New Zealand seeking accession to the Budapest Convention.

43 By acceding to the Budapest Convention, some victims' interests would be better protected. For example, law enforcement agencies would be better able to locate and prosecute child exploitation networks through enhanced international cooperation.

Environmental effects

44 There would be no environmental effects associated with accession.

Te Tiriti o Waitangi / Treaty of Waitangi implications

45 The decision to accede to the Budapest Convention, and the way this decision is implemented, must uphold the Crown's obligations under Te Tiriti o Waitangi / the Treaty of Waitangi.[10]

46 A preliminary hui was held in January 2020 to ascertain Māori interests in the Convention. It confirmed that the nature of the Budapest Convention touches on issues of significance for Māori: including criminal law, search and surveillance, digital inclusion, human rights, and New Zealand's international obligations.

47 The hui 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 legislation such as the Search and Surveillance Act 2012 and the Mutual Assistance in Criminal Matters Act 1992.[11]

48 This paper is intended to provide further information on the benefits and impacts of accession. The Department of the Prime Minister and Cabinet and Ministry of Justice will also undertake targeted consultation with interested parties.

49 As cybercrime data is limited, we do not know whether Māori are disproportionately represented in cybercrime statistics (as either victims or perpetrators). It is also unclear what percentage of Māori individuals or businesses have suffered financial losses from cybercrime and the impact of such losses.

50 The vast majority of the powers required for New Zealand to accede to the Convention, such as search warrants, are already available under New Zealand law.

51 Potential impacts of legislative and operational changes include:

[10] For the avoidance of doubt, there are no specific references to Māori perspectives in the Convention. It has not been involved in a historical or contemporary Treaty claim.

[11] The hui also identified a number of issues which are relevant to a broader policy conversation in the cybersecurity area. It was agreed that further conversation is needed around broader questions on how Māori are included in discussions on cyber security, data sovereignty and digital inclusion more generally. The Department of the Prime Minister and Cabinet will take forward those conversations as part of its overall approach to implementing the Cyber Security Strategy 2019.

a) Data preservation orders can be used to require entities that hold specific information relevant to a specific criminal investigation to preserve that information temporarily on their systems, while a production order is sought to access that information. The addition of surveillance device warrants to the Mutual Assistance in Criminal Matters Act could make a slightly expanded range of information available to foreign agencies for use in criminal investigations. We are interested in your views on whether these changes may interact with wider Māori data sovereignty interests. This is not a new issue raised by accession and it is likely to be more appropriately addressed in a broader context. However, it is a consideration that will be taken into account as far as possible in this context.

b) Māori are disproportionately represented in the criminal justice system. Again, this is a broader issue for the criminal justice system. We are interested in your views on whether there are any opportunities to minimise any disproportionate effect on Māori when making changes required by the Convention to existing processes.

Economic effects

52 A large portion of cybercrime, such as frauds and scams, causes economic loss for businesses, government and individuals. Better addressing cybercrime and other crime would reduce the economic loss. While losses from cybercrime can be difficult to quantify, it appears that it is widespread:[12]

a) CERT NZ recorded 3445 cybercrimes in 2018 with over $14.1 million in financial losses. The most common incidents were credential harvesting (stealing passwords), scams and frauds, and unauthorised access. Most of the losses were to individuals and/or small businesses.[13] A Norton report states that in 2016, more than one-third of New Zealand's adult online population was affected by cybercrime; and that 978 million people were affected by cybercrime in 2017.[14]

b) The National Cyber Security Centre has calculated the value of harm it directly prevented in 2018-19 was in excess of $27.7 million.

53 Under-reporting makes the number of cybercrime incidents and the losses they cause difficult to quantify.

Financial implications

54 Accession would have financial implications for the private sector, as a result of implementing preservation orders as per the requirement for accession.

55 Telecommunications companies and government agencies were consulted on the potential costs and practicalities of introducing a data preservation scheme in New Zealand. While the feedback received was supportive of accession in general, concerns

[12] Precisely quantifying the number of incidents and cost of cybercrime is difficult for a range of reasons (including under-reporting; multiple places to go for help; and differing perceptions of what a 'cybercrime' is).
[13] CERT NZ works to support businesses, organisations and individuals affected by cyber security incidents. Reporting is at https://www.cert.govt.nz/about/quarterly-report/summary-report-2018/.
[14] https://us.norton.com/cyber-security-insights-2017. While many global surveys have a wide margin of error, this is still worthwhile as an illustrative example, especially given an overall lack of cybercrime data.

were raised about the cost of establishing systems for and complying with data preservation orders. Responses suggested that the design of the scheme – such as the scope and amount of data subject to an order, and how streamlined Government agency processes were – would affect its costs. Most respondents favoured a cost recovery scheme and some provided models for such a scheme.

56 A draft proposal for a data preservation scheme is outlined in Appendix B, which takes account of feedback received from consultation. Based on that proposal, which is for a tightly constrained scheme, the total aggregated cost for all telecommunications companies, data storage providers and other related affected parties to comply with data preservation orders, is estimated at $15,000 per annum. This cost would vary by year, both overall and for individual affected parties.

57 This estimated cost assumes between 10 and 15 preservation orders will be issued in New Zealand annually. This is based on the number of current mutual assistance cases each year that involve a request for specific information held by a New Zealand entity, and where preservation of that information could avoid the risk that key evidence would be modified or lost while the mutual assistance application is being processed.

58 The estimate assumes that preservation orders would not be used to support domestic law enforcement investigations, for joint investigations with other countries where criminal offending has taken place in New Zealand. This is because the requirements for making a preservation order would be aligned with those for the making of a production order. If agencies have sufficient evidence of a crime, a production order can be issued to compel the provision of relevant information. Given that production orders can be obtained quickly in New Zealand (taking between 8 to 48 hours), we do not foresee preservation orders being used in support of domestic law enforcement investigations (since generally it would make more sense to seek a production order for the information, in a single step).

59 It also assumes that data preservation orders would not be used to support international criminal investigations where information is supplied to law enforcement and regulatory agencies on request in appropriate circumstances (in line with the Privacy Act), because production orders are not used in these cases.

60 The cost of responding to a preservation order is estimated at an average of $1,000. This cost could include time and resources spent on receiving and checking an order; processing capacity to copy and store the data; and other compliance and staffing costs. It is assumed that that the majority of preservation order requests would be straightforward, with a low cost. A minority are more complex, with a higher cost (for example involving larger volumes of data or data extraction by a specialist engineer).

61 For requests from foreign countries, given that there is no data preservation scheme in place at present, telecommunications companies or data storage providers sometimes preserve relevant information for mutual assistance cases on a voluntary basis, at the request of NZ Police, or directly at the request of the foreign country, in accordance with New Zealand's privacy law, before a production order is issued. In other cases, information is provided through a production order without prior preservation. Therefore it is assumed

that not all of this estimated cost would be an additional cost on companies, compared to the status quo.

62 Further consultation will take place with the telecommunications sector and law enforcement agencies to refine the above assumptions and estimates. Further work is required to consider the appropriate allocation of those costs, once estimates are further refined.

63 There would be some costs to the Crown related to travel, policy work on the legislative changes required, and operational implementation of the changes.

Overall Evaluation

64 At the moment, the Department of the Prime Minister and Cabinet and Ministry of Justice consider that the advantages of the Budapest Convention far outweigh the disadvantages. However, we are keen to hear your views.

65 The Convention sets down a best practice approach that is adopted by all member states. This includes the careful consideration of how human rights are impacted. Any legislative requirements completed by the Ministry of Justice would be assessed for human rights impacts. The Crown Law Office would also conduct a New Zealand Bill of Rights Act review. Accession would improve international co-operation on crime in a variety of contexts and serve New Zealand's long-standing interests.

66 Significantly, accession to the Convention will help our agencies better identify, respond and prevent cybercrime ultimately make New Zealand a safer digital environment for its citizens.

67 This assessment will be reviewed following public feedback on the impacts of accession.

What happens next?

68 The process of accession to the Budapest Convention is managed by the Committee of Ministers of the Council of Europe. It is customary for states which are not members of the Council of Europe, and which wish to join the Budapest Convention, to request an invitation to accede. The Council of Europe then considers the request. If it is accepted, an invitation will then be issued.

69 New Zealand has expressed an interest in acceding to the Budapest Convention to the Council of Europe Secretariat and we are awaiting an invitation to be issued. Expressing an interest to accede is not a binding treaty action.

70 Once we have received an invitation, New Zealand will have 'invited party' status with the Council of Europe. 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. New Zealand would need to complete all steps necessary to accede, (including parliamentary treaty examination and passage of implementing legislation) within this time.

71 Invited party status would provide New Zealand with some immediate benefits ahead of accession, including the ability to attend Budapest Convention meetings as an observer. This includes an upcoming Plenary on the Second Additional Protocol to the Budapest Convention, where discussion will be held on the cooperation on lawful access to evidence held in the cloud, the ability for relevant agencies to cooperate directly with service providers in other countries, improved mutual legal assistance for electronic evidence, and safeguards including around data protection.

72 The Government will consider whether to proceed with accession by late 2020. This decision will be informed by the consultation process.

73 If the Government decides to proceed, the Convention text and a National Interest Analysis would be presented for Parliamentary Treaty Examination. Once presented, the Government must refrain from taking binding treaty action until the relevant select committee has reported or fifteen sitting days have elapsed.[15]

74 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.

Further opportunities for engagement

75 There will be a number of further opportunities to engage in the process, if the Government decides to proceed with joining the Budapest Convention:

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

b) During the implementation process, especially the drafting of implementing legislation, officials will continue targeted engagement with interested civil society groups and with Māori, if there is an identified need.

c) Amendments to the Budapest Convention are governed by Article 44. Any party can propose an amendment. The Secretary-General of the Council of Europe would circulate the proposed change. After all parties have accepted the amendment, the Committee of Ministers would adopt these changes and they would come into force. Amendments to the Convention do not automatically apply to state parties. Any future binding treaty actions, including accession to Additional Protocols, would require Cabinet approval, which would be sought at the appropriate time.

d) There is currently one Additional Protocol to the Convention, "concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems." The Minister of Justice has directed work on hate speech in New Zealand. Assessment of whether New Zealand should accede to this Protocol, and what steps would need to be taken, would be undertaken as part of that work programme.

e) Negotiations between parties to the Convention are also currently underway (expected to end late 2020) on an Additional Protocol on evidence in the cloud, to help law enforcement secure evidence on servers in foreign, multiple or unknown jurisdictions. A Protocol like this would further benefit New Zealand law enforcement.

[15] If no recommendation requiring further government action is required, the parliamentary treaty examination process is complete when the select committee presents its report.

Consideration of whether to accede to this protocol would be subject to engagement prior to any Cabinet decision.

What do you think?

Submissions are invited from all interested parties. Targeted consultation will also take place with Māori, civil society and with the telecommunications industry as part of this process.

Feedback received through consultation will be summarised in and inform the Department of Prime Minister and Cabinet's and Ministry of Justice's advice to the Government on whether New Zealand should proceed to accede to the Budapest convention. It will also support consideration of the legislative changes necessary to implement the Budapest Convention.

You may wish to consider the following questions:

1. Do you have any comments on the assessment of advantages, implications and costs outlined in this consultation paper?

2. Can you provide any further information to support the assessment of advantages, implications and costs?

3. Do you see any risks from joining? Could those risks be mitigated, and if so, how?

4. If New Zealand were to accede, is there anything that you think needs to be taken into account when New Zealand considers how to implement the requirements of the Budapest Convention in its own legislation?

5. If New Zealand were to accede, do you have any comments on the issue of establishing jurisdiction in relation to Convention offences, as required by Article 22(1)(d), and the matter of whether to seek a reservation to this article, as outlined at paragraph 36 of the Consultation paper?

6. Do you have any comments on the policy intent for and/or the detail of the data preservation scheme (such as the conditions for issuing an order), as included at Appendix B?

7. Taking all factors into account, do you agree or disagree that New Zealand should proceed to join the Budapest Convention? In either case, please explain why.

8. Do you have any other comments?

Making a submission

We welcome your feedback on this consultation document. The questions posed throughout this document are summarised in the section above. They are a guide only and all comments are welcome. You do not have to answer all the questions.

How to make a submission

- To make a submission, you can download a copy of the submission form to complete and return to us. This is available on the Ministry of Justice's website. Please email your completed form to budapest@justice.govt.nz.
- If you'd prefer not to use the submission form, you can email your submission to budapest@justice.govt.nz.
- Submissions open on Wednesday 15th of July and close on Friday 11th September, 2020.

Contact for queries

Please direct any queries to budapest@justice.govt.nz

Please note your submission will become official information. This means that the Ministry of Justice may be required to release all or part of the information contained in your submission in response to a request under the Official Information Act 1982.

The Ministry of Justice may withhold all or parts of your submission if it is necessary to protect your privacy or if it has been supplied subject to an obligation of confidence.

Tell us if you think there are grounds to withhold specific information in your submission. The reasons for this might include that it is commercially sensitive, or that it's personal information. Any decision to withhold information can be reviewed by the Ombudsman, who may tell us to release it.

Appendix A: Detail of proposed legislative changes

1 The following are proposals for consultation and are not government policy.

2 To bring New Zealand law into line with the Budapest Convention, the following changes would be required.

Addition of data preservation orders

3 A scheme for data preservation orders would be added to the Search and Surveillance Act. Data preservation orders would require entities that hold specific information relevant to a specific criminal investigation to preserve that information temporarily on their systems, while a production order is sought. (Production orders are a legal instrument under the Search and Surveillance Act requiring an entity to produce requested material within a certain timeframe).

4 Details of the proposed data preservation scheme are attached at Appendix B. The proposed scheme has been based on the recommendations made by the Law Commission in its 2017 report on the Search and Surveillance Act 2012. The report recommended that New Zealand consider a tightly constrained preservation scheme that complies with the Budapest Convention, but does not extend significantly beyond those requirements.

5 Data preservation orders could be issued by law enforcement agencies to any person or entity that is in possession or control of computer data. The data subject to a preservation order would be a discrete set of data relevant to a specific criminal investigation. It would only apply to data that is stored in the normal course of business. Law enforcement agencies would only be able to view or take possession of the data once a production order for that information is obtained.

6 Preservation orders would be of use in cases where overseas agencies become aware of data that is stored in New Zealand relevant to specific criminal investigations they are pursuing. In such cases, there is a relatively lengthy mutual assistance process that needs to be completed before a court can issue a production order (typically 6 to 18 months), and the information can be provided to the overseas counterpart). This process ensures that all relevant domestic legal and human rights issues can be considered appropriately before a court order is sought to have the information provided. However it creates a risk that the data could be modified or lost in the intervening period, in the normal course of business. A preservation order would ensure the data is still there by the time a production order is obtained.

7 In the proposed scheme, the conditions for issuing a preservation order would align with those for issuing a production order under the Search and Surveillance Act, as recommended by the Law Commission. Since the conditions would be aligned, and given the speed at which production orders can be secured in New Zealand (between 8 to 48 hours), this means that preservation orders are unlikely to be frequently used in support of domestic law enforcement investigations (since generally it would make more sense to seek a production order for the information, in a single step).

8 The tightly constrained design of the proposed scheme also means that preservation orders would not be able to be used in some circumstances where electronic information relevant to domestic investigations is vulnerable to loss or modification. The proposed model could not be used if investigations have not reached the stage of affirming sufficient evidence to apply for a preservation order or production order, for example in the early stages of an investigation. This could include investigations for what may later turn out to be serious crimes, such as missing persons and deceased persons, that later become investigations of homicides, other serious crimes and/or a Coroner's inquiry.

Addition of third party confidentiality orders

9 Third party confidentiality orders, for surveillance device warrants and preservation orders, would be added to the Search and Surveillance Act 2012. These would require third parties who are aware of the execution of a surveillance device warrant or preservation order to keep this confidential. This would take effect only while the investigation is taking place, and only if the investigation were to be jeopardised by the disclosure of the order.[16]

10 Third party confidentiality orders would aid law enforcement officers in keeping their investigations confidential in the evidence-gathering stage of an investigation. The individual would not be charged at this stage of the investigation. Once a charge has been made against the individual, they would be notified.

Adjustments to New Zealand's domestic mutual assistance law

11 Surveillance device warrants would be added to New Zealand's mutual assistance law, so they could be used in New Zealand to obtain information relevant to overseas investigations, and vice versa. This would fulfil a reciprocal obligation to assist other countries in return for better access to data held in other countries for New Zealand law enforcement.

12 These changes would be an incremental extension of assistance already available through mutual assistance provisions, and would reflect powers already available for domestic criminal investigations.

13 They would also be subject to the robust safeguards in the Mutual Assistance in Criminal Matters Act (for example, protections against discrimination[17]); and provisions in the Budapest Convention on due process, territorial sovereignty, and requiring human rights protections of its states party.

14 The Mutual Assistance in Criminal Matters Act would also be amended to clarify a power in the Search and Surveillance Act. The power allows the New Zealand government to delay notifying a party affected by a search warrant if, for example, it would jeopardise

[16] Data preservation orders are described in the previous section. Surveillance device warrants give officers the power to, for example, 'wiretap' phone calls and conduct video surveillance on private premises.

[17] The Mutual Assistance in Criminal Matters Act includes a range of mandatory and discretionary grounds for refusing assistance at s27. The mandatory grounds include requests relating to political offences; requests made for prosecuting a person on a range of prohibited grounds such as colour, race, sex and religion; and requests where the person has already faced trial for the same offence (double jeopardy).

an ongoing investigation. The amendment would clarify that this power applies to search warrants issued under the Mutual Assistance in Criminal Matters Act.

15 While this amendment is not strictly required for accession, it directly influences the effectiveness of the mutual assistance New Zealand provides. It is a minor amendment clarifying a statutory interpretation.

16 A similar amendment regarding production orders may be required (for the avoidance of doubt) confirming that notification of an affected party is not required in the mutual assistance context.

Other changes

17 Minor changes would be made to some elements of our computer crime offences. This includes:

a) amendment of section 251 to include language that captures other types of computer crime;

b) explicitly prohibiting making software that is principally to be used for computer crime;

c) prohibiting importation of software that would enable cybercrime.

18 An Order in Council would be made prohibiting the import of a physical device (hardware) for a computer crime.

19 There may be other minor technical consequential amendments associated with the proposed legislative change.

Appendix B: Proposed data preservation scheme

Proposed data preservation scheme for New Zealand

1. The following is a proposed scheme for data preservation orders in the Search and Surveillance Act 2012 (the Act).

2. This document should be read alongside the consultation paper, which provides additional context about the limited circumstances in which the data preservation scheme is likely to be used.

3. These are proposals for consultation purposes. The final scheme implemented may be different from the indicative scheme below. The provisions below would be implemented through provisions in the Search and Surveillance Act 2012 and through operational policy and procedures.

4. The Office of the Privacy Commissioner will be consulted on the proposed scheme to ensure it is consistent with New Zealand's Privacy Framework.

Data preservation scheme: policy intent

5. This data preservation scheme has been developed in line with the requirements of the Council of Europe's Budapest Convention on Cybercrime (the Convention), and particularly the corresponding recommendations on data preservation made by the Law Commission in its 2017 review of the Search and Surveillance Act 2012.

6. The Convention requires us to 'adopt such legislative and other measures as may be necessary to … obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification'. Articles 16, 17, 30, and 31 of the Convention set out further specific detailed requirements.

7. The proposed scheme:

    a. enables law enforcement agencies to make preservation orders under the Search and Surveillance Act 2012, requiring entities to temporarily preserve specific information relevant to a specific criminal investigation while a production order is sought;

    b. supports international criminal investigations and prosecutions involving electronic evidence, thereby improving investigation capability and international cooperation;

    c. is closely aligned with recommendations of the Law Commission's 2017 report, with the requirements for making a preservation order mirroring those for making a production order;

d. ensures that the privacy and human rights of New Zealanders are upheld, as is appropriate in the context of serious crime investigations and existing mechanisms under the Search and Surveillance Act 2012; and

e. enables ease of implementation and administration for both law enforcement agencies and for recipients of preservation orders.

8. This data preservation scheme will not interfere with or modify requirements and operational use of production orders under the Search and Surveillance Act 2012. It will not interfere with or modify arrangements whereby information can be preserved by and/or supplied to law enforcement and regulatory agencies in appropriate circumstances if requested, in line with the Privacy Act. The proposed model does not include consideration of the public/private distribution of costs for investigative tools for serious crimes under the Search and Surveillance Act or the Privacy Act.

Agencies that could apply for preservation orders

9. Agencies that can currently apply for production orders, and therefore would be able to apply for preservation orders under this proposed scheme, include:

- Department of Conservation;
- Department of Internal Affairs (Digital Safety Group);
- Inland Revenue Department.
- Land Information New Zealand;
- Ministry for Primary Industries:
- Ministry for the Environment;
- Ministry of Business, Innovation, and Employment;
- Ministry of Foreign Affairs and Trade;
- Ministry of Health;
- Ministry of Transport;
- New Zealand Customs Service;
- Oranga Tamariki;
- NZ Police;
- Reserve Bank of New Zealand; and
- The Treasury.

Who and what data the scheme would apply to

10. A preservation order could be issued to any person in possession or control of specified computer data.

11. The scheme would apply to any computer data that is **stored**, i.e. non-transient and held for some period, in the normal course of business. This could apply to both content data and metadata.

12. The orders would not apply to data that is not kept for some period, i.e. long enough to 'snapshot' it. This distinguishes preservation orders from surveillance device warrants, which are for continuous collection as opposed to 'snapshotting'.

13. Unlike production orders, which may be used prospectively under the Search and Surveillance Act 2012, the scheme would **not allow for prospective** preservation (i.e. an ongoing obligation to collect and preserve data coming in after the date of the order).

Offences

14. The offences in relation to which a preservation order can be made, would mirror those applicable for the making of production orders. This would mean that preservation orders would generally be available in respect of criminal offences punishable by imprisonment.

Issuing an order

15. The statutory power to make a preservation order would sit with the chief executive of the agencies empowered to seek the orders. As a matter of practice, it is expected this power will be delegated to suitably qualified and responsible officials, in accordance with s 17 of the Policing Act 2008 and s 41 of the State Sector Act 1988. The issuing officer in each agency will only be able to issue a preservation order when satisfied that all relevant statutory conditions are met.

16. The proposed **conditions** for an order to be issued would be based on those made by the Law Commission in their report on the Search and Surveillance Act. The Law Commission recommended that a preservation order can only be issued if the decision-maker is satisfied that:

    a. the relevant enforcement agency intends to apply for a production order in respect of the identified data; and

    b. the issuing officer is satisfied that the requirements for obtaining a production order, including under section 72 of the Search and Surveillance Act, are likely to be met in the circumstances of the case; and

    c. preservation is necessary because the data is vulnerable to loss or modification.

17. The data which is subject to the preservation order is expected to be the same as that for the subsequent production order, as far as can be determined at the time (i.e. not significantly wider or narrower). This is aimed at reducing compliance cost burden on the recipient of an order.

18. **Verbal** orders could be made by an issuing officer when the above criteria are met and where:

    a. there are reasonable grounds to believe it is immediately necessary for an order be made because the data is particularly vulnerable to loss or modification;

    b. it is not practicable in the circumstances to make the order in writing; and

    c. a written record is made of the data preservation order as soon as practicable.

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

20. Data preservation orders would be added to section 175 of the Search and Surveillance Act. Section 175 makes it an offence for a person to make an application for an examination order, production order, search warrant, surveillance device warrant, or declaratory order that contains information they know to be false.

21. There would be **no specific formatting requirements** for the preservation of the data during the time it is preserved by the recipient. Data is not provided to a law enforcement agency until a production order is issued. It is generally expected that information later provided to agencies via a production order will be in usable formats.

Duration of the orders and arrangements for extension

22. The **duration** of the orders would be 30 days for domestic orders, or 180 days for foreign orders. These orders are extendable indefinitely, at each extension for a period not exceeding 30 days (for domestic orders) and 180 days (for foreign orders). Any standard data preservation forms should include the date of expiry of the order.

23. The criteria for extension would be:

    a. the assistance is still required; and

    b. the investigation is ongoing; and

    c. any reasons for delay are explained.

24. The agency issuing the order is **required to serve notice discontinuing** the order if:

    a. the grounds upon which the order was made no longer exist; or

    b. the investigation to which the order relates is otherwise discontinued.

25. If the order is discontinued, or its time period lapses and a production order/extension request is not received, data is subject to the normal requirements of the Privacy Act. This may result in the data being deleted by the data-holder in the normal course of business.

Penalties

26. The penalty for non-compliance with a preservation order would be broadly similar to that for non-compliance with a production order – that is a maximum $40,000 fine for a body corporate and no more than one year imprisonment for an individual.

Other aspects of scheme design required by the Budapest Convention

27. If the investigation the preservation order relates to would be compromised by the order being disclosed, the order can require that the party carrying it out **keep it confidential**. As a matter of practice, this would apply in most cases. This is a requirement of the Budapest Convention.

28. **There would be an enabling provision** for Article 17 of the Budapest Convention. Article 17 relates to circumstances where multiple service providers have been involved in the transmission of information that is the subject of a preservation order. Article 17 requires service providers, upon receipt of a preservation order, to supply New Zealand law enforcement agencies with enough traffic data to identify service providers and the path through which the data was transmitted. Traffic data is a subset of computer data, and is defined in the Budapest convention as data "relating to a communication… generated by a computer system that formed a part in the chain of communication".

Arrangements for international preservation orders

29. Certain law enforcement agencies would be empowered to receive and action **incoming** data preservation requests (as a part of the Search and Surveillance Act 2012 scheme – not mutual assistance legislation). This would mean that agencies would receive and assess a preservation request, and if it met the necessary conditions, issue a preservation order. It is still being considered whether all agencies with domestic preservation order powers would be empowered to receive and action incoming foreign requests or only a subset of those agencies.

30. Arrangements for international orders would align with those for domestic orders. The **conditions** for issuing an international order would be the same as those for issuing a domestic order. This means that New Zealand would only be able to action international preservation requests comply with our domestic laws (including our human rights laws). The conditions for verbal orders, who within each agency can approve the carrying out of the order in New Zealand, and discontinuing the order and/or destroying data, would apply to international requests as they do to domestic orders.

31. In addition, international orders would only be implemented when there is:

    a. an assurance the country intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data; and

    b. sufficient information as to the entity making the order, and confirmation that they have the legal authority to submit the request; and

c. information on who or what entity holds the data, or sufficient information to identify this.

32. As allowed for in the Budapest Convention, we would retain the discretion to refuse to action an incoming order where:

    a. the preservation order relates to political offences (criminal offences directed against a government, e.g. treason; and, in some cases, an 'ordinary' crime with a political element, e.g. assault with a political character), or

    b. where execution of the order is considered likely to prejudice New Zealand's sovereignty, security, public order or other essential interests.

33. In making preservation orders on behalf of another country, New Zealand law enforcement agencies will be required to provide the requesting country with traffic data it receives from service providers in certain circumstances. In particular, where a service provider in another State was also involved in the transmission of a communication, and the traffic data is necessary to identify service providers and the path through which the data was transmitted. New Zealand law enforcement agencies will not be required to supply the information if it refuses to action an incoming order for the reasons outlined at paragraph 32 above.

Guidance and reporting

34. Officials would develop the following operational measures to make the process of applying for an order efficient and consistent:

    a. a standard written form for preservation orders issued in New Zealand, across government agencies (including orders giving effect to international requests);

    b. a process for how agencies receive and action data preservation requests from other countries;

    c. information packs on the scheme to provide to telecommunications companies and other affected parties, and law enforcement agencies, when it is introduced; and

    d. guidance to support requesting countries in making requests that meet New Zealand's legislative requirements and can be implemented expeditiously.

35. There would be Parliamentary annual reporting on how many preservation orders are issued each year by each government agency for any agency that makes more than 100 preservation orders per annum.