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

MINISTRY OF JUSTICE
Tāhū o te Ture

Proactive Release

The following Cabinet paper and related Cabinet Minutes have been prepared for proactive release by the Department of the Prime Minister and Cabinet (DPMC), on behalf of Hon Dr David Clark, Minister for the Digital Economy and Communications, and the Ministry of Justice, on behalf of Hon Kris Faafoi, Minister of Justice:

Council of Europe Convention on Cybercrime:
Approval to Accede

The following documents have been included in this release:

Title of paper: Council of Europe Convention on Cybercrime: Approval to Accede (CBC-20-SUB-0129)

Title of minute: Council of Europe Convention on Cybercrime: Approval to Accede (CBC-20-MIN-0129)

Title of minute: Report of the Cabinet Business Committee: Period Ended 18 December 2020 (CAB-21-MIN-0001)

Some parts of this information release would not be appropriate to release and, if requested, would be withheld under the Official Information Act 1982 (the Act). Where this is the case, the relevant section of the Act that would apply has been identified. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

This Paper contained two attachments which have not been included in publication. Attachment 1: *Council of Europe Convention on Cybercrime (Budapest Convention) (ETS No. 185 23.XI.2001)* can be found online at: https://rm.coe.int/1680081561.
Attachment 2: *National Interest Analysis* will be presented to the House of Representatives in due course.

Key to redaction codes:

- 6(a), to protect the security or defence of New Zealand or the international relations of the Government of New Zealand;
- 9(2)(f)(iv), to maintain the confidentiality of advice tendered by or to Ministers and officials; and
- 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.

Office of the Minister of Justice
Office of the Minister for the Digital Economy and Communications

Chair, Cabinet Business Committee

Council of Europe Convention on Cybercrime: Approval to Accede

Proposal

1 This paper seeks agreement for New Zealand to accede to the Council of Europe Convention on Cybercrime, also known as the Budapest Convention on Cybercrime (hereafter 'the Convention'). It provides a report back on public consultation and final advice on legislative and financial implications, following Cabinet's 'in principle' decision on accession in June 2020.

Executive Summary

2 Cybercrime and cyber-enabled crime cause substantial financial and social harms in New Zealand. Investigating and prosecuting those and other serious crimes has become more challenging, particularly in a cloud computing age, where an offender may be located in one country, the victim in another, and the evidence of the offence held or controlled by a company in a third country.

3 The Budapest Convention aims to improve cooperation on cross-border investigations and prosecutions by providing a consistent framework for defining computer crimes, enabling lawful access to evidence, and outlining expectations on how relevant international agencies assist each other. Signed in 2001, it now has 65 Parties. New Zealand is now an outlier amongst like-minded countries in not having acceded to the Convention.

4 Accession would enhance cooperation with other countries to address cybercrime. It would have reputational value and support wider priorities, including the countering violent extremism work programme that was developed in response to the terror attack in Christchurch in 2019. It would situate New Zealand alongside international partners in the global dialogue to address this global problem – allowing us to participate in shaping the future of a rules-based international order for this area.

5 Consultation has reinforced that accession to the Convention would benefit New Zealand in addressing cross-border crime and protecting copyright. However, Māori groups and individuals consulted expressed reservations about accession. This paper proposes that officials work with Māori to explore the development of a review or oversight mechanism that provides for ongoing Māori involvement in New Zealand's implementation of and participation in the Convention. This would help address some of these concerns and provide an opportunity for continued dialogue on the Convention and its potential future developments.

6 New Zealand's legislative framework largely aligns with the requirements of the Convention. The main change would be the introduction of preservation orders to the Search and Surveillance Act 2012. The Convention requires that Parties have the power to order the preservation of data, giving authorities time to seek its disclosure. Preservation orders mitigate the risk that evidence is modified or deleted before the disclosure process is completed (normally through a production order).

7 The proposed approach is a tightly constrained scheme, based on recommendations made by the Law Commission and the Ministry of Justice in their joint review of the Search and Surveillance Act, completed in 2017. The scheme's primary purpose would be to support

cooperation on international criminal investigations; since, in the absence of a data preservation scheme, the long timeframes for considering mutual assistance requests mean there is a real risk of evidence being modified or lost before the data can be provided to the requesting country.

8 This approach would enable New Zealand to implement the basic framework required for accession quickly, fulfilling one part of a recommendation made by the Royal Commission of Inquiry into the Attack on Christchurch Mosques and delivering on a longstanding cyber security objective.

9 The legislation for accession would not seek to address wider current challenges with enforcing the law in a digital age, nor address the recommendations of the Royal Commission related to reviewing legislative settings related to counter terrorism. Work in these areas will be taken forward separately from the accession process.

10 Subject to satisfactory completion of the Parliamentary Treaty Examination process, legislation would be introduced and passed by the end of 2021, if possible. Accession would be finalised by depositing an Instrument of Accession with the Council of Europe, signed by the Minister of Foreign Affairs.

11 Officials estimate the total cost to industry of compliance with data preservation orders to be in the order of $10,000 to $15,000 per year. These costs are not considered to be materially significant; we propose that these costs are borne by the recipient of the order. There are not anticipated to be material costs associated with the other legislative changes. There will be a range of financial costs to the Crown that will be absorbed within existing baselines.

Background

12 New Zealand's Cyber Security Strategy 2019 identified accession to the Convention as a key area of focus to proactively tackle cybercrime [CAB-18-MIN-0127]. In June 2020, Cabinet made an 'in principle' decision to accede to the Convention, with consideration of full policy decisions in late 2020 [CAB-20-MIN-0252].

13 The Convention is the only international treaty seeking specifically to address internet and computer crime. It aims to prevent, deter and detect crimes committed via the internet and other computer networks. It sets out a consistent basic framework for defining computer crimes, enabling lawful access to evidence, and outlining expectations on how relevant international agencies assist each other.

14 The Convention came into force in 2004 and now has 65 member states, predominantly from Europe, but also from Asia, North and South America, Australia and the Pacific. New Zealand is the only country among like-minded partners *6(a)* that has yet to accede.

Analysis

International cooperation is vital because of the cross-border nature of cybercrime

15 As the internet has become a normalised part of everyday life, it has also become a tool for criminal activity. Cybercrime is increasing in New Zealand and causes substantial financial and social harms. CERT NZ recorded 4,740 cyber security incidents in 2019, with over $16.7 million in financial losses. The actual number is likely much higher. The most common incidents were phishing and credential harvesting (stealing passwords), scams and frauds, and unauthorised access. CERT NZ's half-year report from 2020 shows that reports of cyber security incidents have increased by 42% compared to the same time period in 2019.

16 The Ministry of Justice's Crime and Victim Safety Survey 2019 shows that over 320,000 people experienced fraud or cybercrime over a 12-month period. These figures are likely to significantly understate the true level of cybercrime in New Zealand. Recent high-profile attacks against New Zealand companies reinforce the potential impact of cybercrime and underscore the need for up-to-date policy settings to investigate and prosecute such crimes.

17 Evidence of cybercrime and other serious crime is often held electronically by large internet service or cloud computing providers whose platforms are used by criminals. The global nature of the internet means that an offender may be in one country, the victim in another, while the evidence of the offence is held by a company in a third country.

18 Because of that, law enforcement relies on international cooperation to prevent, investigate, and prosecute crimes committed wholly or in part online. This is simplified when countries have consistent laws for how crimes committed online are defined and how agencies can access recorded evidence of crime.

The Convention sets out a consistent framework for defining computer crimes, enabling lawful access to evidence of serious crime, and outlining expectations on how international agencies assist each other

19 The Convention is a "cybercrime" convention in name, but its benefits extend wider. It addresses pure cybercrime, cyber-enabled crime and criminal evidence stored electronically.

20 Parties to the Convention must ensure the following offences are incorporated in their domestic laws:

a. offences against the confidentiality, integrity and availability of computer data and systems;

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 commercial-scale infringements of copyright and theft of intellectual property.

21 The Convention also requires Parties to adopt search and surveillance powers necessary for obtaining electronic evidence of offending, consistent with domestic and international human rights obligations and other safeguards. These include:

a. measures to order the expeditious preservation of subscriber data, traffic data and content data[1];

b. measures to order the production of specified computer data and subscriber information;

c. measures to enable search and seizure of stored computer data; and

d. measures to collect traffic data associated with specified communications in real-time, and, in relation to serious offences, measures to collect computer content data in real time.

[1] Subscriber data means information that identifies the person using a service, such as their name, account details, address, telephone number, billing and payment information. Traffic data means data relating to the communication, such as its destination, origin, route, time, date, size, duration or type of underlying service. Content data means the content of the communication in question, such as a message, email, image or social media post.

22 The Convention includes provisions explicitly requiring that enforcement powers and procedures established under the Convention are to be conducted with respect for fundamental human rights and freedoms, such as freedom of expression and protection of privacy and personal data.

23 The Convention sets out several principles and procedures related to international cooperation. These include:

a. procedures relating to mutual assistance and the collection and sharing of electronic evidence; and

b. the establishment of a 24/7 designated point of contact to ensure the provision of assistance between parties for the investigation of cybercrime.

24 Each member state determines how to implement the overarching framework in the context of its constitutional arrangements and its privacy and security policies.

Accession to the Convention would enhance cooperation with member states to address cybercrime

25 New Zealand would need to make incremental changes to legislation to accede to the Convention. These changes would complement and enhance New Zealand's existing international cooperation on cybercrime.

26 Member states also share threat trends information, best practice technical advice, and capability-raising initiatives. Accession would give New Zealand access to this. Parties benefit from a global network of points of contact available 24/7.

27 New Zealand would also join negotiations among the member states on enhancements to the Convention to better address cybercrime, such as a Second Additional Protocol to the Convention, which is looking at improving the efficiency of mutual assistance processes and alternative approaches to cooperation on securing electronic evidence.

28 *9(2)(f)(iv)* [redacted]

Accession would have reputational value and support wider priorities

29 Accession would support New Zealand's objectives for a free, open and secure internet. Our absence from the Convention places us outside the evolving norms for international governance of cyberspace. Joining would send a signal that we are committed to like-minded efforts to combat cybercrime, while at the same time protecting fundamental human rights and freedoms. *6(a)* [redacted]

30 In addition, accession signals that our regulatory settings on cybercrime are broadly consistent with like-minded countries. This supports domestic and foreign investment in our digital economy to occur with confidence.

9(2)(f)(iv) [redacted]

31 New Zealand's accession is a key deliverable of both the 2019 Cyber Security Strategy and the countering violent extremism work programme that was developed in response to the terror attack in Christchurch in 2019. The Royal Commission of Inquiry into the Attack on Christchurch Mosques (the Royal Commission) has also recommended that New Zealand accede to and implement the Convention.

Accession to the Convention does not address all the challenges of responding to cybercrime or securing electronic evidence in a digital age, nor implement recommendations of the Royal Commission to review wider legislative settings

32 The nature of technology and criminal activity has changed since the Convention was drafted. Further cybercrime-related policy issues will require consideration over time, outside of the accession process. These include:

a. the long timeframe for mutual assistance;

b. the volatility of electronic evidence;

c. the need for rapid access to data in emergencies; and

d. the increasing use of encryption.

33 At the same time, New Zealand's domestic policy framework has also become dated. The digital environment continues to evolve and legislation, tools and settings need to be reviewed to ensure they are fit for purpose, to enable agencies to better manage and respond to cybercrime.

34 We propose to move quickly to implement the basic framework required to accede to the Convention. That will provide immediate benefits and fulfil part of one recommendation of the Royal Commission (to accede to and implement the Convention).

35 Officials will report back to relevant Ministers in *9(2)(f)(iv)* with a proposed work programme responding to the recommendations made by the Royal Commission of Inquiry into the Attack on Christchurch Mosques to review legislation related to the counter-terrorism effort. *9(2)(f)(iv)*

36 As noted above, the current negotiations on the Second Additional Protocol to the Convention also seek to address some of the issues listed at paragraph 32. New Zealand is attending these negotiations as an observer. Any decision to accede to this protocol would be subject to a separate Cabinet decision process, as would a decision on whether to accede to the existing Additional Protocol to the Convention, which concerns the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Accession would require Parliamentary Treaty Examination and implementing legislation

37 Following Cabinet's 'in principle' decision, the then Minister of Foreign Affairs wrote to the Council of Europe expressing New Zealand's interest in accession. The Committee of Ministers of the Council of Europe responded in October 2020 inviting New Zealand to accede. New Zealand has five years to complete all steps necessary to accede before this invitation lapses.

38 If approved by Cabinet, the attached National Interest Analysis would be presented to the House of Representatives for Parliamentary Treaty Examination. Following completion of this, implementing legislation would be introduced to Parliament.

39 If the legislation is passed, New Zealand can then deposit an Instrument of Accession with the Council of Europe, noting any reservations or declarations (paragraph 63 has further details on reservations available under the Convention). It would be signed and sealed by the Minister of Foreign Affairs. Depositing the Instrument of Accession would be a binding treaty action.

Legislative implications

New Zealand already largely complies with the Convention's requirements

40 If New Zealand were to accede to the Convention, incremental legislative amendments would be required to bring New Zealand law into line.

41 To comply with the obligations under the Convention we are proposing legislative amendments that would introduce a preservation order scheme, third party confidentiality orders, add surveillance device warrants and production orders into the mutual assistance legislation, and make some other minor changes to computer crime offences.

A tightly constrained data preservation scheme would be implemented, the primary purpose of which would be to support cooperation on international investigations

42 The Convention requires parties to have powers to order the preservation of data, giving authorities time to seek its disclosure. Preservation orders mitigate the risk that evidence is modified or deleted before the disclosure process is completed (normally through a production order).

43 The Law Commission and the Ministry of Justice completed a joint review of the Search and Surveillance Act in 2017, including recommendations about the kind of preservation order scheme that should be instituted as part of accession to the Convention. That review concluded that the primary purpose of such a scheme should be to address the known issue of evidence potentially being destroyed while requests from overseas jurisdictions for mutual legal assistance are in process. Requests for mutual legal assistance can take months or even years to complete before Police are authorised to seek a production order from the court. This delay is not an issue that arises in domestic investigations. Production orders can be obtained quickly from the courts when an investigation is sufficiently advanced that the legislative requirements for obtaining an order can be met. Nevertheless, the review concluded that the power should be available for domestic investigations, on the principle that we should not make tools available internationally that are not available domestically.

44 An alternative approach is to implement an expanded preservation order scheme that would have a greater use in domestic investigations, by allowing preservation earlier in the investigative process. This option would require further policy work and has the potential to create significant additional compliance costs for business. It would also require further

consultation with stakeholders. Therefore, we propose to implement a tightly constrained preservation scheme for the purpose of accession, aligned with the Law Commission and Ministry of Justice recommendations, as outlined below. *9(2)(f)(iv)* [redacted]

45 Preservation orders would be a new power in the Search and Surveillance Act 2012. The purpose of preservation orders would be to require a person that holds specific information relevant to a criminal investigation to preserve that information temporarily on their systems when an application for a production order or a request for mutual legal assistance is about to be made or has been made, but has not yet been granted or refused.

46 The power to issue a preservation order would be given to the Commissioner of Police. The power could be delegated by the Commissioner of Police, in accordance with section 17 of the Policing Act 2008. The Commissioner would be able to issue a preservation order at the request of any enforcement agency that is entitled to apply for a production order under the Search and Surveillance Act 2012.[3] This approach – rather than enabling those agencies to issue preservation orders directly – was recommended by the Law Commission to assist in ensuring that the regime was administered efficiently and effectively, given the low volume of orders anticipated. It ensures a consistent approach to oversight.

47 The conditions for issuing a preservation order would be aligned with those for issuing a production order. The Commissioner of Police could issue a data preservation order when they are satisfied that:

a. the relevant enforcement agency is about to apply for or has applied for a production order, in respect of the identified data;

b. the requirements for obtaining a production order are likely to be met; and

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

48 With an international request for data preservation, these conditions would be met when the relevant international agency has confirmed they are about to submit or have submitted a mutual assistance request for the specified data, and provided an outline of the offence that is the subject of the investigation, the related facts of the case and the necessity of preservation. This approach is based on the requirements of the Convention for making international requests and is intended to provide a quick and efficient process for preserving data that is the subject of an incoming mutual assistance request.

49 The duration of preservation orders would be 20 days for domestic investigations, with no ability to extend the orders because a production order can normally be obtained very quickly in New Zealand. The duration of orders would be 150 days for international orders, with a limit of four 180-day extensions. Preservation orders could only require the preservation of information which is already held (i.e. there would be no ability to use an order to proactively preserve information which has not yet come into the possession of the data-holder).

50 The offences in relation to which a preservation order can be made would mirror those for the making of production orders. The penalty for non-compliance would also be aligned with the penalty for production orders (maximum of $40,000 fine for a body corporate and no

[3] s 71(1) of the Search and Surveillance Act provides that "enforcement officers who may apply for a search warrant to obtain documents" are eligible to apply for production orders. 51 Acts administered by 15 different agencies include powers to seek search warrants for documents, including those administered by NZ Police, the Department of Internal Affairs, Customs, the Ministry of Primary Industries and Inland Revenue.

more than one year's imprisonment for an individual). Orders would be able to be appealed to the district court (on any aspect of the order).

51 Preservation orders would also require the recipient to disclose a limited amount of traffic data to Police, to address circumstances where multiple service providers[4] were involved in the transmission of a communication. In those cases, it might be necessary to issue multiple preservation orders to different recipients, in order to ensure that the full information sought is ultimately preserved. The disclosure of limited traffic data upfront, without requiring a production order, facilitates this process. This is required by the Convention, for both domestic and international orders (Articles 17 and 30).

52 This arrangement meets the requirements of the Convention while ensuring that, in the domestic context, the power does not create demand for unnecessary or low-value preservation orders, or otherwise interfere with law enforcement applying for production orders in a timely way.

53 New Zealand Police would designate a point of contact available on a 24/7 basis, to provide immediate assistance to other countries on investigations or proceedings, coordinating with other agencies as required. This role will include the receipt and issuing of data preservation orders to support mutual assistance requests.

Third party confidentiality orders would be introduced, requiring data holders to keep the execution of preservation orders, production orders or surveillance device warrants confidential

54 The Convention requires the ability to oblige a service provider (such as a telecommunications company or cloud computing provider) to keep the execution of a preservation order or surveillance device warrant confidential. This guards against the risk of the investigation being jeopardised by the disclosure of the existence of the order or warrant.

55 The Convention does not require confidentiality in respect of production orders (although the explanatory notes on the Convention do encourage states to consider this measure). However, investigations are equally likely to be jeopardised by the disclosure of the existence of a production order as with a preservation order or search warrant. There is also a risk that if confidentiality orders are only available for preservation orders, but not for production orders, that it could undermine timely applications for production orders, and could create an unintended incentive to use preservation orders.

56 We propose to provide for confidentiality orders in respect of preservation orders, production orders, and surveillance device warrants. The specific terms of any confidentiality obligation would need to be set out in the relevant order or warrant, but would provide that both existence of the order/warrant itself be kept confidential, along with any other personal information that would not have been collected or retained but for the existence of the order.

57 The confidentiality obligations would cease when a preservation order lapses (where no production order had subsequently been issued in respect of the information), or at the end of an investigation in the case of a production order or a surveillance device warrant. The enforcement agency that sought the order would have a positive obligation to notify any service providers who are subject to an obligation of confidence when an investigation has ended. At that point, the normal Privacy Act principles would apply.

58 A person who intentionally breaches the requirements of a confidentiality order would be subject to a penalty.

[4] A service provider is defined as any public or private entity that provides the ability to communicate by means of a computer system, or the processing or storage of data

Surveillance device warrants and production orders would be added to mutual assistance

59 Surveillance device warrants and production orders would be made available in support of incoming mutual assistances requests. This would also make it possible for New Zealand to request the use of such powers from other countries in support of outgoing requests.

60 We are proposing to carry over all the usual safeguards that apply domestically to the handling and use of information obtained by way of a surveillance device warrants, with the appropriate modifications. The introduction of surveillance device warrants and production orders into mutual legal assistance arrangements would not affect the Court's control over the issuing and monitoring of the warrants and orders.

Other minor changes would be required

61 Existing offences in the Crimes Act 1961 and the Customs and Excise Act 2018 would be clarified to explicitly criminalise the "production", "procurement for use" and "importation" of devices and information intended to be used for committing a specified cybercrime offence.

The legislative changes would primarily have an impact on the private sector

62 The above legislative changes would primarily impact the digital sector, specifically telecommunications companies, internet service providers and cloud computing providers. That is because those entities sometimes hold communications data or user-generated data that can be evidence of a crime. The financial impact on these sectors should be minor, given the low number of preservation orders expected to be issued per year (around 10-15 in support of international investigations, and very few or none in support of domestic investigations). The sector has been consulted on the proposed scheme (see paragraph 84 below).

We propose to invoke two reservations to the Convention to ensure consistency with our broader legislative settings

63 The Convention allows for reservations to nine articles, of which we propose to invoke two. These are to reserve the right:

a. not to provide for the availability of surveillance device warrants to intercept traffic data associated with lower-level offences that are punishable by a term of imprisonment of less than 7 years, as allowed for under Article 14(3)(a) of the Convention; and

b. not to extend our criminal jurisdiction to cover the criminal actions of New Zealanders committed wholly outside of New Zealand, where we do not already establish extraterritorial jurisdiction for the offence, as allowed for under Article 22(2) of the Convention (relating to the application of Article 22(1)(d)).

Legislative process matters

64 The proposals in this paper require amendments to the Search and Surveillance Act 2012, the Mutual Assistance in Criminal Matters Act 1992, the Crimes Act 1961, and the Customs and Excise Act 2018 to have legal effect. Policy responsibility for these changes falls primarily within the Justice portfolio, therefore the Minister of Justice would lead on the necessary policy and legislative decisions. The necessary amendments would be made through an omnibus Bill, with an overall theme of bringing New Zealand law into line with the legislative requirements of the Convention prior to accession.

65 The 2020 Legislation Programme includes the Accession to the Council of Europe Convention on Cybercrime Bill, 9(2)(f)(iv) The Minister of Justice is seeking approval to issue drafting instructions to Parliamentary counsel as soon as Cabinet has agreed to the policy decisions being sought.

66 The Minister of Justice will submit a legislative bid for the 2021 Legislation Programme, 9(2)(f)(iv)

67 The Minister of Justice is also seeking authorisation to take further detailed policy decisions for the purpose of drafting legislation to implement the requirements of the Convention, subject to those details being consistent with the overall direction of this paper, and following consultation with relevant Ministers. 9(2)(f)(iv)

68 The Bill will be binding on the Crown. The Search and Surveillance Act 2012, the Mutual Assistance in Criminal Matters Act 1992, the Crimes Act 1961, and the Customs and Excise Act 2018 are all binding on the Crown.

Financial implications

69 Officials estimate the total cost of compliance with data preservation orders to be between $10,000 and $15,000 per year. This is based on officials' estimate that compliance with a preservation order would cost an average of $1000, with between 10-15 orders issued per year. This relatively low estimated cost is because orders are expected to be used only in support of mutual assistance requests which are seeking production of information that could be vulnerable to modification or loss during the mutual assistance process. These costs are not considered to be materially significant. During consultation, telecommunications companies submitted that the costs of data preservation would be higher than those outlined and supported a cost recovery scheme, while data storage providers who submitted noted that the costs are likely to be already incorporated into the costs of doing business or may be less than $1000 per order.

70 A cost recovery scheme is unlikely to be justified for the proposed preservation order scheme. It would be inefficient and potentially out of step from a wider policy perspective to create a cost recovery scheme for what is a relatively low compliance burden when spread across the industry. Therefore, we propose that these costs are borne by the recipient of the order.

71 There are not anticipated to be material costs associated with the other legislative changes.

72 There will be a range of financial costs to the Crown that will be absorbed within existing baselines. These include costs associated with policy and implementation work on legislative changes, attendance at council meetings, implementing the 24/7 'point of contact' function and the issuing of preservation orders.

73 The proposal to establish a review or oversight mechanism for ongoing Māori involvement in the Convention (paragraph 89 refers) may have associated financial implications, but it is too early to quantify these. Officials will report back to the Minister for the Digital Economy and

9(2)(f)(iv)

Communications and the Minister of Justice on this, after initial work with Māori to explore possible options.

Impact analysis

74 The Ministry of Justice and the Department of the Prime Minister and Cabinet have prepared a National Interest Analysis (NIA), which is attached. The Regulatory Quality Team at the Treasury has determined that a separate Regulatory Impact Statement is not required for the regulatory proposals in this paper because it would substantively duplicate the National Interest Analysis. The exemption is granted on the condition that the document contains all the requirements that would be otherwise be included in the Regulatory Impact Statement.

75 The Ministry of Justice QA Panel has reviewed the National Interest Analysis: The Council of Europe Convention on Cybercrime, prepared by the Ministry of Justice and the Department of the Prime Minister and Cabinet. The Panel considers that the information and analysis summarised in the NIA contains most of the requirements that would be otherwise be included in the RIA. The Panel considers that these sections of the NIA partially meet the quality assurance criteria for a RIA (complete, convincing, clear and concise, and consulted).

76 The NIA demonstrates good stakeholder consultation on acceding to the treaty, and responsiveness to stakeholder concerns. However, given the context in which the NIA is being prepared, the examination of alternative options to the treaty, and the impacts and benefits of these alternative options, is minimal. This may make it difficult for Ministers to assess the potential value of the non-treaty alternatives to addressing the issues identified in the NIA. Notwithstanding, the Panel found the arguments put forward for accession to the treaty to be compelling.

Climate Implications of Policy Assessment

77 The Climate Implications of Policy Assessment (CIPA) team has been consulted and confirmed that the CIPA requirements do not apply to this proposal, as the threshold for significance is not met.

Application to Tokelau

78 Officials will consult with Tokelau on whether it would like New Zealand's accession to the Convention to extend to Tokelau.

Population implications

79 Improved ability to cooperate with other countries on cybercrime, cyber-enabled crime and other serious crime will have population-wide benefits.

80 Māori are overrepresented in the criminal justice system. As cybercrime data is incomplete, it is not known whether Māori are disproportionately represented in cybercrime statistics (as either victims or perpetrators). Given the limited legislative changes required for accession, it is unlikely that accession to the Convention will affect in any way the existing overrepresentation of Māori in the criminal justice system.

81 Officials do not consider it likely that this proposal would give rise to any specific impacts on women, people who are gender diverse, children, veterans, Pacific peoples, rural communities or ethnic communities. However, due to the limitations of cybercrime data, it is hard to draw definitive conclusions about the impacts on specific groups of an improved ability to cooperate with other countries on cybercrime.

Human rights

82 The Convention includes provisions that explicitly require enforcement powers and procedures established under the Convention to be conducted with respect for fundamental human rights and freedoms, such as freedom of expression and protection of privacy and personal data.

83 Cooperation under the Convention is subject to the conditions provided for in domestic law, including the grounds on which a country may refuse to provide mutual assistance. The Mutual Assistance in Criminal Matters Act 1992 provides mandatory and discretionary grounds to refuse requests for assistance; these grounds protect human rights.

Public consultation

84 The Ministry of Justice and the Department of the Prime Minister and Cabinet ran a formal public consultation process from July to September 2020. Consultation focused on the proposal that New Zealand accede to the Convention and the details of the preservation order scheme. An information session was held for the telecommunication and cloud storage sectors. Drawing on the guidance established by the Te Arawhiti framework for Crown engagement with Māori and the 2001 Strategy for Engagement with Māori on International Treaties, officials consulted with Māori groups and organisations who were thought to have an interest in the proposals.

85 Seventeen written submissions were received, from telecommunications companies and membership organisations, cloud computing companies, civil society organisations, Māori groups and organisations and from individuals (commenting from the perspective of civil society, digital privacy and Māori data sovereignty) and from the Privacy Commissioner.

86 Most submitters supported accession to the Convention. Submitters acknowledged that accession would be a benefit to New Zealand in addressing international crime, as well as protecting copyright.

87 We received three submissions from Māori groups and individuals and had a small number of meetings and phone calls. Most Māori groups and individuals that we heard from expressed reservations about accession to the Convention at this time. Concerns were expressed that international interests may be put ahead of the Treaty of Waitangi, that accession could exacerbate the overrepresentation of Māori in the criminal justice system, and that accession could create risks for the protection of Māori data. Some submitters proposed a role for Māori in governance and oversight, to mitigate the above risks. There was a keenness to build on the discussions to date and for further dialogue on a range of cyber security policy matters.

88 Some of the feedback received from Māori consultation touched on wider questions about the Māori–Crown relationship in the criminal justice area, including proposals for Māori involvement in specific criminal investigations. These are broader questions that cannot be adequately addressed through the accession process. Officials do not believe that accession to the Convention will foreclose future developments between the Crown and Māori on the evolving relationship within the criminal justice system or on specific measures to eliminate overrepresentation. The Convention gives flexibility for countries to implement its provisions in a way that is appropriate for their constitutional context.

89 However, we consider it would be appropriate to explore whether a mechanism could be established to allow for an ongoing review or oversight role for Māori in the implementation of and participation in the Convention. This could take the form of a review process to allow ongoing dialogue about the impact of and benefits of accession in practice. It could also

provide a means for working with Māori on future developments in the Convention. We will discuss what form this could take with those we consulted, and keep options open at this stage to whether this is a separate process focussed on the Convention, or could be taken forward as part of a broader conversation on cyber issues or through the central Māori–Crown dialogue on criminal justice. This approach is in line with the Government's commitments to strengthen the Māori-Crown relationship, to ensure that the Crown can grow to be a better Treaty Partner and work in true partnership with Māori.

90 Feedback from consultation has informed the final policy design of the data preservation scheme.

Consultation on the Cabinet paper

91 This paper was prepared by the Ministry of Justice and the Department of the Prime Minister and Cabinet. The following agencies have been consulted on this paper, the attached NIA or other preparatory work: Crown Law, the Department of Internal Affairs, the Ministry of Business, Innovation and Employment, the New Zealand Customs Service, the Ministry of Foreign Affairs and Trade, the New Zealand Intelligence Community, New Zealand Police, Stats NZ, Te Arawhiti, Te Puni Kōkiri, The Treasury and the Serious Fraud Office.

6(a), 9(2)(g)(i) - NZ Police

6(a), 9(2)(g)(i) - DPMC and MoJ

6(a), 9(2)(g)(i) - DPMC and MoJ

9(2)(f)(iv), 9(2)(g)(i), 9(2)(h) - Crown Law

Comment from the Privacy Commissioner

97 The Office of the Privacy Commissioner has been consulted. The Privacy Commissioner recognises there are considerable benefits for New Zealand from accession to the Convention. He considers it is possible to obtain the benefits of accession without unnecessarily intruding on individual privacy rights. He remains concerned about the following aspects of the legislative regime proposed to accede to the Convention:

- that the application for a preservation order does not align with that of a production order (i.e. no judicial oversight is required);
- individuals will be unable to seek redress without a positive obligation on agencies to advise individuals following the expiration of an order; and
- the proposal to extend the confidentiality of preservation orders to the production order regime when this is not required by the Convention.

98 Officials will continue to work with the Office of the Privacy Commissioner during the legislative drafting process.

Communications

99 Cabinet's decision to accede to the Convention will be confirmed by a press statement, with timing determined by the Ministers of Justice and for the Digital Economy and

Communications, in consultation with the office of the Minister of Foreign Affairs and the Prime Minister's Office. Reactive talking points and Q&As will be provided to Ministers.

Proactive release

100 This paper will be proactively released on the Ministry of Justice's website, subject to any necessary redactions justified in accordance with the Official Information Act 1982.

Recommendations

101 The Minister of Justice and the Minister for the Digital Economy and Communications recommend that the Committee:

1 **Note** that in June 2020 Cabinet agreed in principle to accede to the Council of Europe Convention on Cybercrime, subject to further consultation, and detailed advice on legislative changes required for and financial implications of accession [CAB-20-MIN-0252 refers];

2 **Note** that, following a formal expression of interest by the Minister of Foreign Affairs in June 2020, the Committee of Ministers of the Council of Europe invited New Zealand to accede to the Convention in October 2020, and that the invitation is valid for five years;

3 **Agree** that New Zealand accede to the Council of Europe Convention on Cybercrime (the Budapest Convention), subject to the satisfactory completion of the Parliamentary Treaty Examination process;

4 **Approve** the content of the National Interest Analysis, which is attached to the paper;

5 **Agree** to present the text of the Council of Europe Convention on Cybercrime and the National Interest Analysis to the House of Representatives for the purposes of the Parliamentary Treaty Examination process, under Standing Order 405;

6 **Note** that officials will consult with Tokelau on whether it would like New Zealand's accession to the Convention to extend to Tokelau;

7 **Note** that New Zealand's accession will be brought into effect by the deposit of an Instrument of Accession, following completion of Parliamentary Treaty Examination and passage of implementing legislation;

8 **Authorise** the Minister of Foreign Affairs to sign and deposit New Zealand's Instrument of Accession in accordance with Article 37 of the Convention, once all domestic steps necessary to accede have been completed;

Data preservation orders

9 **Agree** that the Search and Surveillance Act 2012 be amended to introduce data preservation orders, the purpose of which would be to require a person that holds specific information relevant to a criminal investigation to preserve that information temporarily on their systems when an application for a production order or a request for mutual legal assistance is about to be made or has been made, but has not yet been granted or refused;

10 **Agree** that:

a. the power to issue a preservation order would sit with the Commissioner of Police;

b. the Commissioner of Police would be able to issue a preservation order at the request of any enforcement agency that is entitled to apply for a production order under the Search and Surveillance Act 2012;

11 **Agree** that the Commissioner of Police could issue a data preservation order when they are satisfied that:

a. the relevant enforcement agency is about to apply for or has applied for a production order, in respect of the identified data;

b. the requirements for obtaining a production order are likely to be met; and

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

12 **Agree** that, with an international request for data preservation, these conditions would be met when the relevant international agency has confirmed they are about to submit or have submitted a mutual assistance request for the specified data, and provided an outline of the offence that is the subject of the investigation, the related facts of the case and the necessity of preservation;

13 **Agree** that the duration of preservation orders would be:

a. 20 days for domestic orders, with no ability to extend the orders;

b. 150 days for international orders, with the ability for the issuing officer to extend the order by an additional 180 days, up to four times;

14 **Agree** that the offences in relation to which a preservation order can be made, and the penalty for non-compliance, would mirror those for the making of production orders;

15 **Agree** there would be a right of appeal to the District Court by the recipient of a preservation order on any aspect of the order;

16 **Agree** that a person be required to disclose limited traffic data upon receipt of a preservation order, for the sole purpose of achieving the requirements of Article 17 and Article 30 of the Convention;

17 **Agree** that New Zealand Police report annually on numbers of preservation orders made and any other relevant information about the exercise of the preservation order power;

Other changes required in order to accede

18 **Agree** to provide for surveillance device warrants and production orders to be made available in support of mutual assistance requests;

19 **Agree** that the safeguards that apply domestically to the handling and use of information obtained by way of a surveillance device warrant would also apply, with the necessary modifications, when used in support of mutual assistance requests;

20 **Agree** to provide for third party confidentiality orders, which would impose an obligation of confidentiality on service providers who are aware of the execution of a preservation order, production order, or surveillance device warrant;

21 **Agree** that confidentiality orders will require that the existence of the order or warrant itself be kept confidential, and that any personal information that would not have been collected or retained but for the existence of the order or warrant be kept confidential;

22 **Agree** that confidentiality obligations should cease when a preservation order lapses or at the end of an investigation in the case of a production order or a surveillance device warrant;

23 **Agree** that a person who intentionally breaches the requirements of a confidentiality order would be subject to a penalty;

24 **Agree** that existing offences in Crimes Act 1961 and the Customs and Excise Act 2018 be clarified to explicitly criminalise the "production", "procurement for use" and "importation" of devices and information intended to be used for committing a specified cybercrime offence;

25 **Note** that New Zealand Police will designate a point of contact available on a 24/7 basis, to provide immediate assistance to other countries on investigations or proceedings, coordinating with other agencies where appropriate;

Reservations

26 **Agree** to invoke reservations to the Convention:

a. to reserve the right not to provide for the availability of surveillance device warrants to intercept traffic data associated with lower-level offences that are punishable by a term of imprisonment of less than 7 years, as allowed for under Article 14(3)(a) of the Convention; and

b. to reserve the right not to extend our criminal jurisdiction to cover the criminal actions of New Zealanders committed wholly outside of New Zealand, where we do not already establish extraterritorial jurisdiction for the offence, as allowed for under Article 22(2) of the Convention (relating to the application of Article 22(1)(d)).

Financial implications

27 **Note** that the total cost to telecommunications companies and other affected parties to comply with data preservation orders is not expected to be materially significant;

28 **Note** that there will be financial costs to the Crown associated with policy and implementation work on the legislative changes, attending Convention meetings, implementing the 24/7 'point of contact' function and the issuing of preservation orders, which would be absorbed within existing agency baselines;

Legislative implications

29 **Note** that the 2020 Legislation Programme includes an omnibus Bill to bring New Zealand law into line with the legislative requirements of the Budapest Convention, 9(2)(f)(iv) ;

30 **Note** that the Minister of Justice will submit a bid for the 2021 Legislation Programme of the same nature, 9(2)(f)(iv) ;

31 **Invite** the Minister of Justice to issue drafting instructions to the Parliamentary Counsel Office to give effect to the policy proposals above;

32 **Authorise** the Minister of Justice to take further detailed policy decisions for the purpose of drafting legislation to implement the requirements of the Convention, subject to those details being consistent with the overall direction of this paper, and following consultation with relevant Ministers;

33 9(2)(f)(iv) ;

34 **Note** that the recommendations with drafting implications are subject to Parliamentary Counsel's discretion concerning how best to express these in legislation.

Responding to feedback from Māori consultation

35 **Note** that some submitters proposed a role for Māori in governance or oversight of the Convention and its mechanisms;

36 **Agree** that officials will work with Māori to explore the development of a review or oversight mechanism that provides an avenue for ongoing Māori involvement in New Zealand's implementation of and participation in the Convention;

37 **Note** that officials will report back to the Minister for the Digital Economy and Communications and the Minister of Justice on a review or oversight mechanism, including any associated financial implications;

Broader related work

38 **Note** that DPMC and MOJ will report to relevant Ministers in 9(2)(f)(iv) with a proposed legislative work programme responding to the recommendations made by the Royal Commission of Inquiry into the Attack on Christchurch Mosques to review legislation related to the counter-terrorism effort;

39 9(2)(f)(iv) ;

Publicity & Proactive Release

40 **Note** that Cabinet's decision to accede to the Convention will be confirmed by a press statement, with timing determined by the Ministers of Justice and for the Digital Economy and Communications in consultation with the Prime Minister's Office; and

41 **Note** that this Cabinet paper is to be published on the Department of the Prime Minister and Cabinet's website, subject to any necessary deletions justified in accordance with the Official Information Act 1982.

Authorised for lodgement

Hon Kris Faafoi
Minister of Justice

Hon Dr David Clark
Minister for the Digital Economy and Communications

ATTACHMENT 1: COUNCIL OF EUROPE CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION) (ETS No. 185 23.XI.2001)

Separate document

Attachment 1 not included in the publication of this Cabinet material. Document can be found online at: https://rm.coe.int/1680081561

ATTACHMENT 2: NATIONAL INTEREST ANALYSIS

Separate document

Attachment 2 has not been included in this release and will be presented to the House of Representatives in due course.

Cabinet Business Committee

Minute of Decision

Council of Europe Convention on Cybercrime: Approval to Accede

Portfolios **Justice / Digital Economy and Communications**

On 16 December 2020, the Cabinet Business Committee, having been authorised by Cabinet to have Power to Act [CAB-20-MIN-0536]:

Accession

1 **noted** that on 2 June 2020, Cabinet agreed in principle to accede to the Council of Europe Convention on Cybercrime (the Budapest Convention), subject to further consultation, and detailed advice on legislative changes required for and financial implications of accession [CAB-20-MIN-0252];

2 **noted** that, following a formal expression of interest by the Minister of Foreign Affairs in June 2020, the Committee of Ministers of the Council of Europe invited New Zealand to accede to the Budapest Convention in October 2020, and that the invitation is valid for five years;

3 **agreed** that New Zealand accede to the Budapest Convention, the text of which is attached to the paper under CBC-20-SUB-0129, subject to the satisfactory completion of the Parliamentary Treaty Examination process;

4 **approved** the content of the National Interest Analysis, attached to the paper under CBC-20-SUB-0129;

5 **agreed** to present the text of the Budapest Convention and the National Interest Analysis to the House of Representatives for the purposes of the Parliamentary Treaty Examination process, under Standing Order 405;

6 **noted** that officials will consult with Tokelau on whether it would like New Zealand's accession to the Convention to extend to Tokelau;

7 **noted** that New Zealand's accession will be brought into effect by the deposit of an Instrument of Accession, following completion of Parliamentary Treaty Examination and passage of implementing legislation;

8 **authorised** the Minister of Foreign Affairs to sign and deposit New Zealand's Instrument of Accession in accordance with Article 37 of the Convention, once all domestic steps necessary to accede have been completed;

Data preservation orders

9 **agreed** that the Search and Surveillance Act 2012 be amended to introduce data preservation orders, the purpose of which would be to require a person that holds specific information relevant to a criminal investigation to preserve that information temporarily on their systems when an application for a production order or a request for mutual legal assistance is about to be made or has been made, but has not yet been granted or refused;

10 *9(2)(f)(iv)* [redacted]

11 **agreed** that:

11.1 the power to issue a preservation order would sit with the Commissioner of Police;

11.2 the Commissioner of Police would be able to issue a preservation order at the request of any enforcement agency that is entitled to apply for a production order under the Search and Surveillance Act 2012;

12 **agreed** that the Commissioner of Police could issue a data preservation order when they are satisfied that:

12.1 the relevant enforcement agency is about to apply for or has applied for a production order, in respect of the identified data;

12.2 the requirements for obtaining a production order are likely to be met; and

12.3 preservation is necessary because the data is vulnerable to loss or modification;

13 **agreed** that, with an international request for data preservation, these conditions would be met when the relevant international agency has confirmed they are about to submit or have submitted a mutual assistance request for the specified data, and provided an outline of the offence that is the subject of the investigation, the related facts of the case and the necessity of preservation;

14 **agreed** that the duration of preservation orders would be:

14.1 20 days for domestic orders, with no ability to extend the orders;

14.2 150 days for international orders, with the ability for the issuing officer to extend the order by an additional 180 days, up to four times;

15 **agreed** that the offences in relation to which a preservation order can be made, and the penalty for non-compliance, would mirror those for the making of production orders;

16 **agreed** that there would be a right of appeal to the District Court by the recipient of a preservation order on any aspect of the order;

17 **agreed** that a person be required to disclose limited traffic data upon receipt of a preservation order, for the sole purpose of achieving the requirements of Article 17 and Article 30 of the Convention;

18 **agreed** that New Zealand Police report annually on numbers of preservation orders made and any other relevant information about the exercise of the preservation order power;

Other changes required in order to accede

19 **agreed** to provide for surveillance device warrants and production orders to be made available in support of mutual assistance requests;

20 **agreed** that the safeguards that apply domestically to the handling and use of information obtained by way of a surveillance device warrant would also apply, with the necessary modifications, when used in support of mutual assistance requests;

21 **agreed** to provide for third party confidentiality orders, which would impose an obligation of confidentiality on service providers who are aware of the execution of a preservation order, production order, or surveillance device warrant;

22 **agreed** that confidentiality orders will require that the existence of the order or warrant itself be kept confidential, and that any personal information that would not have been collected or retained but for the existence of the order or warrant be kept confidential;

23 **agreed** that confidentiality obligations should cease when a preservation order lapses or at the end of an investigation in the case of a production order or a surveillance device warrant;

24 **agreed** that a person who intentionally breaches the requirements of a confidentiality order would be subject to a penalty;

25 **agreed** that existing offences in Crimes Act 1961 and the Customs and Excise Act 2018 be clarified to explicitly criminalise the 'production', 'procurement for use' and 'importation' of devices and information intended to be used for committing a specified cybercrime offence;

26 **noted** that New Zealand Police will designate a point of contact available on a 24/7 basis, to provide immediate assistance to other countries on investigations or proceedings, coordinating with other agencies where appropriate;

Reservations

27 **agreed** to invoke reservations to the Convention:

27.1 to reserve the right not to provide for the availability of surveillance device warrants to intercept traffic data associated with lower-level offences that are punishable by a term of imprisonment of less than 7 years, as allowed for under Article 14(3)(a) of the Convention; and

27.2 to reserve the right not to extend New Zealand's criminal jurisdiction to cover the criminal actions of New Zealanders committed wholly outside of New Zealand, where New Zealand does not already establish extraterritorial jurisdiction for the offence, as allowed for under Article 22(2) of the Convention (relating to the application of Article 22(1)(d));

Financial implications

28 **noted** that the total cost to telecommunications companies and other affected parties to comply with data preservation orders is not expected to be materially significant;

29 **noted** that there will be financial costs to the Crown associated with policy and implementation work on the legislative changes, attending Convention meetings, implementing the 24/7 'point of contact' function and the issuing of preservation orders, which would be absorbed within existing agency baselines;

Legislative implications

30 **noted** that the 2020 Legislation Programme includes an omnibus Bill to bring New Zealand law into line with the legislative requirements of the Budapest Convention, 9(2)(f)(iv)

31 **noted** that the Minister of Justice will submit a bid for the 2021 Legislation Programme of the same nature, 9(2)(f)(iv) ;

32 **invited** the Minister of Justice to issue drafting instructions to the Parliamentary Counsel Office to give effect to the policy decisions above;

33 **authorised** the Minister of Justice to take further detailed policy decisions for the purpose of drafting legislation to implement the requirements of the Convention, subject to those details being consistent with the overall direction of the paper under CBC-20-SUB-0129, and following consultation with relevant Ministers;

34 9(2)(f)(iv)

35 **noted** that the above paragraphs with drafting implications are subject to Parliamentary Counsel's discretion concerning how best to express these in legislation;

Responding to feedback from Māori consultation

36 **noted** that some submitters proposed a role for Māori in governance or oversight of the Convention and its mechanisms;

37 **agreed** that officials work with Māori to explore the development of a review or oversight mechanism that provides an avenue for ongoing Māori involvement in New Zealand's implementation of and participation in the Convention;

38 **directed** the Ministry of Justice and the Department of the Prime Minister and Cabinet to report to the Minister of Justice and the Minister for the Digital Economy and Communications by May 2021 on a review or oversight mechanism, including any associated financial implications;

Broader related work

39 **directed** the Department of the Prime Minister and Cabinet and the Ministry of Justice to report to relevant Ministers in 9(2)(f)(iv) with a proposed legislative work programme responding to the recommendations made by the Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques on 15 March 2019 to review legislation related to the counter-terrorism effort;

40 9(2)(f)(iv)

Gerrard Carter
Committee Secretary

Present: (see over)

Present:
Rt Hon Jacinda Ardern (Chair)
Hon Grant Robertson
Hon Kelvin Davis
Hon Dr Megan Woods
Hon Chris Hipkins
Hon Andrew Little
Hon David Parker
Hon Nanaia Mahuta
Hon Poto Williams
Hon Damien O'Connor
Hon Stuart Nash
Hon Kris Faafoi
Hon Dr David Clark
Hon Dr Ayesha Verrall

Officials present from:
Office of the Prime Minister
Department of the Prime Minister and Cabinet

Cabinet

Minute of Decision

Report of the Cabinet Business Committee: Period Ended 18 December 2020

On 26 January 2021, Cabinet made the following decisions on the work of the Cabinet Business Committee for the period ended 18 December 2020:

Out of scope

Out of scope

CBC-20-MIN-0129	**Council of Europe Convention on Cybercrime: Approval to Accede** Portfolios: Justice / Digital Economy and Communications	CONFIRMED

Out of scope

Michael Webster
Secretary of the Cabinet