International treaty examination of the Council of Europe Convention on Cybercrime

Report of the Justice Committee

July 2021

Contents

Ginny Andersen
Chairperson

Council of Europe Convention on Cybercrime

Recommendation

The Justice Committee has conducted the international treaty examination of the Council of Europe Convention on Cybercrime. The committee recommends that the Government consult the Privacy Commissioner on the design of the legislation before it is introduced to Parliament. The committee notes that the Government intends the treaty to be implemented through a bill.

Introduction to the convention

The Council of Europe Convention on Cybercrime—also known as the Budapest Convention—is the only international treaty addressing cybercrime. Cybercrime includes any crime that has an online element, such as malicious software attacks, as well as crime that results in the creation of electronic evidence. The latter may include crimes relating to child sexual exploitation material, terrorism, and fraud, among others.

Currently 65 countries are parties to the convention. They are predominantly from Europe, but include countries from Asia, North and South America, and the Pacific. A further 12 countries are in the process of joining.

The convention seeks to improve cooperation on cybercrime

Crimes with a cyber element can easily span national borders. The convention seeks to increase international cooperation to combat cybercrime by:

- aligning parties' laws on cybercrime
- aligning parties' search and surveillance powers for accessing electronic evidence
- establishing common channels and protocols through which law enforcement agencies can cooperate and share electronic evidence
- facilitating the sharing of best-practice advice and technical information on cybercrime.[1]

Countries that wish to join the convention must implement the convention's provisions in their domestic law before they can formally join. We discuss what this means for New Zealand below.

We note with appreciation that the Council of Europe invited New Zealand to join the convention in October 2020. Implementation of the convention's provisions was also recommended by the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019.[2]

[1] Ministry of Justice and Ministry of Foreign Affairs and Trade, National Interest Analysis - The Council of Europe Convention on Cybercrime, p. 2 (included as Appendix B of this report).

[2] Ko tō tātou kāinga tēnei: Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019, Chapter 2, recommendation 49.

Legislation is necessary to ratify the agreement

The National Interest Analysis (the NIA) prepared by the Ministry of Justice and Ministry of Foreign Affairs and Trade states that, while New Zealand's legislation complies with the majority of the obligations contained in the Convention, some legislative changes will be required.

The NIA identifies that the main legislative changes required would be amendments to the Search and Surveillance Act 2012 and the Mutual Assistance in Criminal Matters Act 1992, to implement the following policies:

- introducing preservation orders that would require a person who holds electronic evidence to ensure that it is not deleted while a production order is sought from the Courts to compel its production
- introducing third-party confidentiality orders that would require those who are called upon to execute a preservation order, production order, or a surveillance device warrant (such as a telecommunications provider) to keep its existence confidential for a period of time while disclosure would prejudice an ongoing investigation
- making surveillance device warrants available to support international investigations.[3]

Further legislative amendments would be needed to the Crimes Act 1961 and the Customs and Excise Act 2018.

The NIA identifies the following as legal obligations resulting from joining the treaty that will require implementation:

a) criminalising cybercrimes (e.g. illegal access to a computer), computer-related crimes (e.g. fraud), and content-related crimes (e.g. child sexual exploitation material), (Articles 2-11);

b) procedural powers to be established, implemented, and applied in a way that adequately protects human rights (Article 15);

c) procedural powers such as preservation, production, search and seizure, and interception of data should be established for the investigation of cybercrime (Articles 16-21);

d) cybercrime offences detailed in the Convention shall be deemed to be extraditable offences between Convention Parties (Article 24); and

e) procedural powers to support mutual legal assistance with other Parties on the preservation, production, search and seizure, and interception of electronic evidence (Articles 25- 35).[4]

The NIA does not discuss whether any change is required to implement obligation (d), regarding extradition. However, we understand that all the offences covered by the convention are considered extraditable offences under New Zealand law as they carry a maximum penalty of 12 months' imprisonment or more.[5] Further, extradition under this

[3] MOJ and MFAT, National Interest Analysis, p. 3 (included as Appendix B of this report).

[4] Ibid., p. 8.

[5] Extradition Act 1999, section 60(1)(e).

convention would be covered by section 60(4) of the Extradition Act 1999. That section covers the extradition of offenders to countries that New Zealand has a multilateral treaty with, for offences specified as extraditable offences in the treaty.

We note that the NIA proposes that New Zealand enter reservations to the convention—meaning the provisions would not apply to New Zealand—on two matters. The first reservation would limit the range of offences for which New Zealand is required to enable the real-time collection of traffic data to only offences that are punishable by a term of imprisonment of seven years or more. The second reservation would limit New Zealand's ability to prosecute New Zealanders who commit cybercrimes outside New Zealand to only the most serious offences, such as terrorism and human trafficking.

We note that the NIA proposes that these legislative changes be made by an omnibus bill.

Privacy Commissioner's submission

We received written evidence and heard oral evidence from the Privacy Commissioner. The commissioner supports New Zealand joining the convention. He did, however, make several recommendations regarding the design of the legislative changes required.

The Commissioner submitted that the power to issue preservation orders should sit with the judiciary rather than the Commissioner of Police. He said that delegating this power to the chief executive of the relevant enforcement agency is "an inappropriate delegation of a power to override New Zealanders' privacy rights".

The Commissioner also recommended that the legislation require that law enforcement agencies notify individuals that their personal information has been subject to a preservation order, production order, or surveillance device warrant. He suggested this could occur either at the conclusion of the relevant investigation or the expiry of the relevant order or warrant, if doing so would not prejudice the maintenance of the law. This would enable people to "exercise their rights of redress in regard to any wrongful or erroneous collection of their personal information".

We recommend that the Government consult the Privacy Commissioner on the design of the legislation before it is introduced to Parliament.

Appendix A

Committee procedure

This treaty was referred to us on 1 June 2021. We met between 3 June and 8 July 2021 to consider it. We called for public submissions with a closing date of 20 June 2021. We received two submissions and heard oral evidence from one submitter. We also heard evidence from the Ministry of Justice and the Ministry of Foreign Affairs and Trade.

Committee members

Ginny Andersen (Chairperson)
Hon Simon Bridges
Simeon Brown
Dr Emily Henderson
Harete Hipango
Nicole McKee
Willow-Jean Prime
Vanushi Walters
Arena Williams

Evidence received

The documents that we received as evidence are available on the Parliament website, www.parliament.nz.

Appendix B

National Interest Analysis

The National Interest Analysis, prepared by the Ministry of Justice and the Ministry of Foreign Affairs and Trade, is attached.

National Interest Analysis

The Council of Europe Convention on Cybercrime

Contents

Executive summary

1. This National Interest Analysis sets out a qualitative analysis of why New Zealand should accede to the Council of Europe Convention on Cybercrime (the Convention). Accession will signal that New Zealand is serious about cooperating with other countries in combating crimes committed or organised online, and in reciprocating international law enforcement cooperation on criminal investigations when required.

2. The Convention is the only international treaty addressing cybercrime. It opened for signature in November 2001, and since that time 65 States have become Parties. A further 12 countries are in the process of acceding.

3. The borderless nature of cybercrime means that it is difficult to detect and prosecute offenders without international cooperation. When offences are committed online it is common for the offender to be located in one jurisdiction, the victim in another, and the evidence of the offence to be held on a server in a third country.

4. The Convention overcomes these problems by:

    a) aligning Parties' laws on cybercrime;

    b) ensuring Parties share similar search and surveillance powers for accessing electronic evidence;

    c) establishing common channels and protocols through which law enforcement agencies can cooperate and share electronic evidence; and

    d) facilitating the sharing of best-practice advice and technical information on cybercrime.

5. The Convention ensures that these powers are designed and applied in a way that upholds fundamental human rights and freedoms, such as the freedom of expression and the protection of privacy and personal data.

6. Cybercrime is increasing in New Zealand every year and causes substantial financial and social harms. The Ministry of Justice's Crime and Victim Safety Survey 2019 shows that over 320,000 people experienced one or more incidents of fraud or cybercrime in the 12 months preceding the survey.

7. At its highest level, cybercrime includes any crime that has an online element, or otherwise results in the creation of electronic evidence. For example, real-world sexual offending that is shared online, or an assault that is livestreamed, are both within the purview of the Convention. Accession will mean that New Zealand is better able to call on international partners to lawfully collect evidence located in their countries, and to share this with law enforcement here.

8. In addition to supporting the international response to cybercrime, a key benefit of accession is that it puts New Zealand in a position to negotiate further agreements that will create the future infrastructure underpinning international criminal justice

cooperation. Accession to the Convention is the gateway through which New Zealand must pass to ensure that future agreements are useful for us and align with our values.[1]

9. The main implication of accession is the need to make some minor changes to New Zealand's domestic legislation. This primarily entails changes to the Search and Surveillance Act 2012 and the Mutual Assistance in Criminal Matters Act 1992. This includes:

    a) introducing preservation orders that would require a person who holds electronic evidence to ensure that it is not deleted while a production order is sought from the Courts to compel its production;

    b) introducing third-party confidentiality orders that would require those who are called upon to execute a preservation order, production order, or a surveillance device warrant (such as a telecommunications provider) to keep its existence confidential for a period of time while disclosure would prejudice an ongoing investigation; and

    c) making surveillance device warrants available to support international investigations.

10. Consultation has been undertaken on the proposal that New Zealand's accedes and on the required legislative changes. Generally, accession was seen as a positive step for New Zealand, with wide-ranging benefits for individuals and companies in New Zealand.

11. The majority of the feedback from consultation was related to a) concerns about the impact that accession could have on the disproportionate representation of Māori in the criminal justice system; and b) the parameters of the data preservation scheme, including concerns about new compliance costs for those who are called upon to execute preservation orders.

12. Overall, we do not consider that accession will increase Māori representation in the criminal justice system. This is because New Zealand's laws already largely align with the requirements of the Convention, and accession will involve minimal changes to existing law enforcement tools and practices. We also assess that the compliance costs are expected to be minimal, and are unlikely to exceed $15,000 total in any year. The remainder of the feedback on the data preservation scheme has been incorporated into the final design.

Nature and timing of the proposed treaty action

13. Accession to the Convention would require that implementing legislation be in place before the Instrument of Accession is deposited. Following the Treaty Examination Process, we propose that implementing legislation be introduced to Parliament and passed by 2021. If the requisite changes are adopted, New Zealand could then deposit an Instrument of Accession with the Council of Europe.

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

[1] For example, negotiations are currently underway on a Second Additional Protocol to the Convention that seeks to respond to the challenges of accessing electronic evidence in the cloud. This Protocol has the potential to significantly reduce the timeframes for the provision of legal assistance and could result in significant changes to how law enforcement agencies cooperate. Accession to any new agreements would be subject to a separate treaty examination process.

Reasons for New Zealand to become Party to the treaty

15. The Convention is the most complete and comprehensive international standard to date for responding to cybercrime. It provides a comprehensive framework that enables law enforcing cooperation, including the sharing of electronic evidence.[2] The Convention underpins the existing mechanisms of international law enforcement cooperation, within which New Zealand already participates.

16. Although a cybercrime convention in name, the Convention is concerned with a wide range of offending. It addresses:

    a) pure cybercrime – criminal acts committed through communication technologies or the internet where the computer or network is the target of the offence (e.g. deploying malicious software). This type of offending can be in service of many different motivations, including financial gain, political influence, or espionage; and

    b) cyber-enabled crime – criminal acts 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 crimes, such as the distribution of child sexual exploitation material, terrorism, and fraud.

Cybercrime is increasing and requires international cooperation

17. Cybercrime has substantial economic and social costs for New Zealand businesses, individuals, and government. The Ministry of Justice's Crime and Victim Safety Survey 2019 shows that over 320,000 people experienced one or more incidents of fraud or cybercrime over the previous 12 months. CERT NZ's yearly report for 2019 shows 689 incidents (15% of all reports) had some sort of financial loss, with a total value of $16.7 million. The National Cyber Security Centre's Cyber Threat Report 2019/20 recorded 352 cyber incidents affecting nationally significant organisations.

18. When offences are committed online it is common for the offender to be located in one jurisdiction, the victim in another, and the evidence of the offence to be held on a server in a third country. Cybercrimes are perpetrated by criminals outside New Zealand who target New Zealanders, and by New Zealanders targeting people overseas. Sometimes evidence occurring wholly overseas is stored by offenders by internet providers located in New Zealand.

19. The Convention overcomes the challenges of international cooperation in responding to cybercrime by:

    a) aligning Parties' laws on cybercrime;

    b) ensuring Parties share similar search and surveillance powers for accessing electronic evidence;

    c) establishing common channels and protocols through which law enforcement agencies can cooperate and share electronic evidence; and

    d) facilitating the sharing of best-practice advice and technical information on cybercrime.

[2] Council of Europe, Acceding to the Budapest Convention on Cybercrime: Benefits, 28 August 2019.

Accession aligns with other Government priorities

20. At a strategic level, accession to the Convention supports New Zealand's broader objectives for a free, open, and secure internet. Accession is a key area of focus in the New Zealand Cyber Security Strategy 2019 (the Strategy). The Strategy has five priority areas to improve cyber security between 2019-2023, including to be 'internationally active' and to 'proactively tackle cybercrime'. Accession to the Convention is listed as a key area of focus to proactively tackle cybercrime, although it will also support our objective of being internationally active, and the Strategy's other priority areas.

21. Accession is also a key deliverable of the countering violent extremism work programme that was approved by Cabinet in response to the terror attack in Christchurch in 2019. It will support international cooperation to address a range of serious offences, including the sharing of terrorist or violent extremist content online.

Major and like-minded Parties to the Convention

22. There are currently 65 members of the Convention, predominantly from Europe, but also from Asia, North and South America, and the Pacific.

23. New Zealand's accession to the Convention would send a strong signal that we are committed to international like-minded efforts to combat cybercrime, while at the same time upholding a rules-based international order which protects fundamental human rights and freedoms, such as freedom of expression and protection of privacy and personal data.

Advantages and disadvantages of accession

24. The main benefits of accession for New Zealand currently are international in nature. This is because the vast bulk of New Zealand law already aligns with the requirements of the Convention. However, accession could lead to a range of secondary domestic benefits should future international criminal justice treaties bring positive changes to existing law enforcement tools or processes. Accession to the Convention is the gateway that New Zealand must pass through to participate in negotiations on these future agreements and to ensure any resulting treaty is useful to us and aligns with our values.

25. The disadvantages are financial in nature. Accession would create new, though extremely marginal, compliance costs for New Zealand industry. We anticipate the monetary cost will be in the order of $15,000 per year total for New Zealand as a whole. Accession will also create new costs for the Crown, though these can be met within baselines.

Accession would enhance international cooperation, both now and in the future

26. New Zealand's accession to the Convention will give us access to networks for the sharing of intelligence on malicious actors, investigatory best practices, and threat trends. Parties to the Convention are automatically made members of the Cybercrime Convention Committee (T-CY), which is a comprehensive intergovernmental body dealing with cybercrime.

27. The T-CY is currently working on a Second Additional Protocol to the Convention covering enhanced international cooperation and access to evidence stored in the cloud. By acceding to the Convention, New Zealand would be able to contribute to the development of this and any future additional Protocols, thus contributing to the further alignment of the international criminal justice infrastructure with our interests.

28. The constantly evolving nature of cybercrime makes it difficult to predict what issues or cases will arise in the future. Importantly, accession to the Convention will ensure New Zealand contributes to and benefits from the collective battle against cybercrime, ultimately making New Zealand's digital environment safer for its citizens.

Accession has reputational and practical value for New Zealand

29. The Convention is seen internationally as a benchmark for laws on cybercrime and access to electronic evidence for law enforcement. Accession signals that our regulatory settings on cybercrime are broadly consistent with like-minded countries, enabling domestic and foreign investment in our digital economy to occur with confidence.

30. The Council of Europe advises that private sector entities are more likely to cooperate with criminal justice authorities of Parties to the Convention. Accession confirms Parties have robust domestic legal frameworks on cybercrime and electronic evidence in place, including the necessary human rights safeguards.[3]

31. The Convention includes provisions explicitly requiring that enforcement powers and procedures established under the Convention are conducted with respect for fundamental human rights and liberties, such as freedom of expression, and protection of privacy and personal data (Article 15: Conditions and Safeguards).

32. The legislative amendments required for New Zealand's accession to the Convention are minor in nature and will result in only modest improvements to our capacity to effectively cooperate internationally. The primary changes required are to the Search and Surveillance Act 2012 and the Mutual Assistance in Criminal Matters Act 1992, in order to:

    a) introduce a scheme for making preservation orders. These will require a person who holds electronic evidence to ensure that it is not modified or deleted while an application for production order (or mutual assistance request from a foreign jurisdiction) has been or is about to be made;

    b) introduce third-party confidentiality orders. These will require those who are called upon to execute a preservation order, production order, or a surveillance device warrant (such as a telecommunications provider) to keep confidential the existence of the warrant for a period of time where disclosure would prejudice an ongoing investigation; and

    c) make surveillance device warrants available to support international investigations.

33. While statutory provisions for enforceable preservation and confidentiality will be new to New Zealand, the practices themselves will not be. The Privacy Act 2020 already allows holders of personal information to voluntarily preserve information that is evidence of criminal and keep confidential that fact in support of a criminal investigation.

[3] For example, companies that hold data such as Internet Service Providers or social media companies.

Accession would result in new but minor compliance costs for industry and the Crown

34. Preservation orders would be a new type of order that would require anyone who holds electronic evidence of criminal offending to preserve that information from loss. Preservation orders would be a precursor to seeking a production order from the Court to authorise law enforcement to access the evidence. In practice, we expect preservation orders will only regularly be served on telecommunication companies and cloud storage providers.

35. Preservation orders will create some new compliance costs for those required to execute them. The costs will include time and resources spent on receiving and executing the order, and the infrastructure to hold the data. The estimated cost of compliance will vary depending on its scope and clarity of each order made. However, we estimate this as an average of about $1,000 per order made,[4] with only 10 to 15 preservation orders made per annum. This latter figure is based on the current number of mutual legal assistance requests that we receive each year seeking data that may be vulnerable to loss or modification.

36. We do not anticipate any regular domestic use for preservation orders. This is because of the speed at which production orders can be obtained from the Court (usually within two days), which significantly reduces the likelihood that data is lost or modified. In contrast, it can take up to two years to consider requests from foreign jurisdictions for mutual legal instance before a production order can be sought from the Courts, during which time it is much more probable that essential evidence could be modified or deleted.

37. In terms of costs to the Crown, accession would create some ongoing costs of servicing international commitments (e.g. reporting on compliance with Convention requirements, and attending T-CY meetings), monitoring and reporting on the implementation of new Search and Surveillance Act powers, as well as operating the 24/7 point of contact function. These costs will be absorbed within existing agency baselines.

Options and overall evaluation

38. As the Convention is the only substantive multilateral treaty enabling international cooperation on cybercrime, the options available to address the issues outlined previously are constrained.

39. If we continue with the status-quo, that is, if New Zealand does not accede to the Convention and does not make any of the requisite legislative changes for compliance:

    a) New Zealand would not be able to shape that strategic direction of international criminal justice architecture that is currently under development. This could ultimately result in New Zealand losing its ability to effectively cooperate with partners over time, or otherwise require that we implement treaties that are not fully aligned with our interests.

    b) New Zealand's international reputation would continue to suffer, as we would not be able to fully contribute to tackling cybercrime in a global context. This could have an impact on our efforts to take leadership on other international endeavours that concern related matters, such as the Christchurch Call.

[4] Feedback from the industry about this estimate has been mixed, but this feedback was not detailed enough to support the development of a better estimate.

c) New Zealand would avoid the modest financial implications of accession – both the compliance costs for industry and the modest operational costs for the Crown.

40. As an alternative to accession to the Convention and implementing the necessary changes to domestic law, New Zealand could seek to pursue a variety of bilateral agreements with our closest partners on international criminal justice cooperation. However, this would likely involve significant resource and would provide less benefit overall. It would likely also be very difficult to achieve, as accession to the Convention is commonly seen as a prerequisite to core capability for international criminal justice cooperation in a way that promotes human rights.

41. Overall, we consider that the advantages of the Budapest Convention far outweigh the disadvantages. The Convention sets down a best practice approach that is adopted by all Parties, including all of our closest partners. Accession would improve international cooperation on crime in a variety of contexts and serve New Zealand's long-standing interests.

Legal obligations resulting from treaty action, the position in respect of reservations, and an outline of any dispute settlement mechanisms

42. The Budapest Convention requires that Parties adhere to a range of procedural provisions on cybercrime, to enable better international cooperation in investigating cybercrime and obtaining electronic evidence for all types of crime.

43. New Zealand's legislation complies with the majority of the obligations contained in the Convention. Some incremental changes will be required to implement these obligations. The substantive obligations can be found in the following provisions:

a) criminalising cybercrimes (e.g. illegal access to a computer), computer-related crimes (e.g. fraud), and content-related crimes (e.g. child sexual exploitation material), (Articles 2-11);

b) procedural powers to be established, implemented, and applied in a way that adequately protects human rights (Article 15);

c) procedural powers such as preservation, production, search and seizure, and interception of data should be established for the investigation of cybercrime (Articles 16-21);

d) cybercrime offences detailed in the Convention shall be deemed to be extraditable offences between Convention Parties (Article 24); and

e) procedural powers to support mutual legal assistance with other Parties on the preservation, production, search and seizure, and interception of electronic evidence (Articles 25- 35).

Reservations to the Budapest Convention

44. Parties can enter reservations for specific provisions of the Budapest Convention, per Article 42. We propose to invoke two reservations to the Convention, those at Article 14(3)(a) and Article 22(2).

45. The reservation to Article 14(3)(a) relates to the application of Article 20, which requires that Parties provide for the real-time collection of traffic data for the offences set out in Articles 2 – 11 of the Convention. The Search and Surveillance Act 2012 does not distinguish between traffic and content data, so a surveillance device warrant would be required to satisfy Article 20. However, a surveillance device warrant can only be obtained in respect to more serious offences (generally those that are punishable by a term of imprisonment of seven years or more). Several of the offences contained at Articles 2 – 11 are at the less serious end of the spectrum. Exercising the reservation at Article 14(3)(a) would ensure that New Zealand is only required to enable the real-time collection of traffic data for more serious offences that are punishable by a term of imprisonment of seven years or more.

46. The reservation at Article 22(2) relates to the application of Article 22(1)(d), which requires that Parties establish jurisdiction over the criminal offences set out in Articles 2 - 11 of the Convention when the offence was committed by a citizen, but occurred wholly overseas. Generally, New Zealand only apply our criminal law extraterritorially in relation to a range of the most serious offences (e.g. terrorism or human trafficking). The offences set out at Articles 2 -11 of the Convention do not meet the threshold of severity to extend jurisdiction.

Dispute settlement mechanisms

47. Article 45 of the Convention outlines the applicable dispute settlement mechanism – Parties would seek a settlement of any dispute between themselves through negotiation managed by the European Committee on Crime Problems. There are no concerns with this body overseeing disputes.

Measures that the Government must adopt to implement the treaty action, including specific reference to implementing legislation

48. If New Zealand is to accede to the Budapest Convention, implementing legislation would be required. New Zealand already largely complies with most of the legislative and regulatory requirements of being a member to the Convention, such as having production orders, surveillance device warrants, and defined computer crime offences.

49. Many of the obligations outlined in the previous section are met by provisions contained in the Crimes Act 1961, the Search and Surveillance Act 2012, and the Mutual Assistance in Criminal Matters Act 1992. There are some minor amendments to these Acts that would be required for accession. Subject to approval, these would be presented to Parliament at the draft Bill stage. They are outlined below.

50. It is proposed that these amendments would take place through an omnibus Bill. This is the preferred option for implementing the obligations of the Budapest Convention. The proposed amendments have no impacts on associated regulations. A Bill will be presented to Parliament following the Parliamentary Treaty Examination process.

51. New Zealand received an invitation to accede from the Council of Europe in October 2020. New Zealand has five years to complete all steps necessary to accede before this invitation lapses.

Search and Surveillance Act 2012

Preservation orders

52. Articles 16, 17, 29 and 30 of the Convention require that New Zealand implement a new search and surveillance tool providing for the preservation of specific electronic evidence of criminal offending. This tool would ensure that:

    a) evidence is not deleted or modified before law enforcement agencies are able to obtain a production order from the court to have that information produced, or while an international request for mutual legal assistance is in the process of being made or considered; and that

    b) a limited amount of 'traffic data'[5] is disclosed to law enforcement agencies so that other relevant service providers can be identified and served with preservation orders if necessary.

53. Currently, the Privacy Act 2020 requires companies to delete personal information that is no longer required for a lawful purpose. The regular deletion of data is a common business practice, particularly when a person closes an account. Offenders commonly close their accounts when they are seeking to conceal or destroy evidence of their offending.

54. The Privacy Act 2020 has an exception that allows companies to voluntarily refrain from deleting personal information in order to avoid prejudicing a criminal investigation. However, this is not enforceable and voluntary preservation is not adequate to meet the requirements of the Convention.

55. Preservation orders would require entities that hold specific information relevant to a specific criminal investigation to temporarily preserve that information 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. Like other search and surveillance powers, a preservation order would override normal Privacy Act obligations.

56. A preservation order scheme was considered by the Law Commission and the Ministry of Justice in its joint review of the Search and Surveillance Act 2012. The review recommended a tightly-constrained preservation which complies with the Budapest Convention but does not extend significantly beyond those requirements.[6]

57. The final design of the data preservation scheme has been based on the Law Commission's recommendations and has been refined through several rounds of consultation with the public and the telecommunications and cloud computing industries, who are most likely to be subject to data preservation orders.

---

[5] Traffic data includes the destination, route, time, date, size, and duration of internet traffic. A preservation order would not permit or require any part of the substantive communication or data being provided to law enforcement without a production order being obtained by the courts.

[6] Report can be found here: https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC-R141-Review-of-the-Search-and-Surveillance-Act-2012-final_0.pdf

Third-party confidentiality orders

58. Third party confidentiality orders would also need to be added to the Search and Surveillance Act 2012. These orders require third parties who are aware of the execution of a surveillance device warrant or preservation order to keep its existence confidential, along with any information that would not have been collected or would have been deleted but for the existence of the order. Confidentially orders would only be available where the disclosure of the information could prejudice an ongoing investigation. The order would lapse when the investigation was completed, for example, if charges were brought or a decision was taken that no offence was committed.

59. The Budapest Convention only requires that such confidentiality orders apply to preservation orders and surveillance device warrants. However, in New Zealand, confidentiality should also apply to the production order for consistency and to ensure that the settings do not incentivise the use of preservation orders before a production order.

Mutual Assistance in Criminal Matters Act 1992

60. An adjustment is required to New Zealand's mutual assistance law, making the device warrants and production orders from the Search and Surveillance Act 2012 available through the Mutual Assistance in Criminal Matters Act 1992. This change would fulfil a reciprocal obligation to assist other countries.

61. 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.

Crimes Act 1961 & Customs and Excise Act 2018

62. Minor changes are required to some elements of our computer crime offences and customs legislation. For example, Article 6 of the Convention requires the criminalisation of a range of actions relating to the possession of, or trade in, devices or information intended to be used for cybercrime. Our laws would need to be updated to specifically criminalise the "production", "procurement for use", and "importation" of these devices or information.

Human rights implications

63. The main human rights implications of the Convention are that it sets out search and seizure. The right to be free from unreasonable search and seizure is affirmed under section 21 of the Bill of Rights Act 1990.

64. Article 15 of the Convention affirms core international human rights instruments and requires that Parties implement the search powers required by the Convention in a way that is consistent with human rights.

65. The legislative changes required for accession do not provide for unreasonable searches. The proposed new powers are justifiable and include appropriate safeguards. For example:

a) judicial authorisation is still required for search warrants, production orders, and surveillance device warrants;

b) preservation orders are only available when, amongst other factors, the requirements of a production order are likely met. This means that the law enforcement agency must have reasonable grounds to suspect that an offence has been committed, and reasonable grounds to believe that the information sought for preservation may constitute evidential material related to the offence; and

c) the gatekeeping role of the Attorney-General and Crown Law in respect of the provision of mutual legal assistance to foreign jurisdictions remains. This gatekeeping role sets out the grounds for refusing to provide assistance in international investigations, such as when the offence is a political in nature or likely to prejudice New Zealand's sovereignty, security, or other essential interest (such as the Crown's obligations to Māori).

66. A formal human rights assessment of the any forthcoming implementation legislation will be completed ahead of legislation being introduced to the House. This includes the Ministry of Justice considering the construction of any new offences and penalties.

Monitoring the impacts of accession

67. There is unlikely to be a quantifiable reduction in cybercrime as a result of accession to the Convention due to the difficulties in measuring this type of crime. This is because: cybercrime is frequently under-reported; the Convention mainly works by improving the response to cybercrime, not stopping it before it happens; and existing New Zealand practice is already largely aligned with the requirements of the Convention.

68. The Convention requires periodic reporting by Parties. This would be an opportunity for New Zealand to review the efficiency and effectiveness of the changes it has made as a result of acceding to the Budapest Convention. In addition, the proposed data preservation scheme includes annual reporting on how many preservation orders are issued each year by New Zealand Police.

Economic, social, cultural and environmental costs and effects of the treaty action

Environmental effects

69. There would be few or no environmental effects from accession.

Cultural effects

70. The decision to accede to the Convention, and the way this decision is implemented, must uphold the principles of the Treaty of Waitangi | Te Tiriti o Waitangi.

71. As cybercrime data is incomplete, it is not known whether Māori are disproportionately represented in cybercrime statistics (as either victims or perpetrators). There is also uncertainty about what percentage of Māori individuals or business have suffered financial losses from cybercrime and the impact of such losses.

72. A preliminary hui was held in January 2020 to ascertain Māori interests in the Convention. Following this, consultation was undertaken with Māori groups and organisations during the public consultation period. As a result of that consultation, the

Māori interests in this issue are understood to concern the criminal justice system, criminal law, search and surveillance, protection of data, copyright, human rights, and upholding Te Tiriti o Waitangi when implementing New Zealand's international obligations.

Criminal justice system, criminal law and search and surveillance

73. The Māori organisations and individuals that we heard from raised the possibility that accession could exacerbate the overrepresentation of Māori in the criminal justice system.

74. Given the limited legislative changes required for accession, we do not consider that accession to the Convention will affect in any way the existing overrepresentation of Māori in the criminal justice system. Further, accession to the Convention provides the opportunity for the Crown to ensure that any future international criminal justice treaties that could result in more significant changes to existing practices adequately protects Māori interests.

75. Accession to the Convention will not foreclose future developments between the Crown and Māori on the evolving relationship within the criminal justice system or on specific measures to eliminate overrepresentation.

Protection of data

76. Some Māori we heard from raised concerns that Māori data may be at risk if New Zealand accedes to the Convention. They noted that for many Māori, data is considered a taonga. While this is a legitimate issue, only data and information held or created by both Māori and non-Māori that contains evidence of offending would be sought by law enforcement agencies under current arrangements or once New Zealand is a member of the Convention.

77. The Convention requires law enforcement agencies be empowered to preserve and obtain specified electronic evidence of particular instances of criminal offending. In New Zealand there is a high legal threshold for law enforcement agencies to obtain this type of information, with access ultimately requiring a court warrant. Accession to the Convention would not change this. These strict legal tests provide the basis for ensuring that data that is not relevant to the specific criminal offending in question would not be provided in response to a mutual assistance request.

78. The Convention does not enable the collection of broad sets of data about populations or communities unrelated to specific criminal offending; it does not enable any type of social profiling.

Copyright

79. The Convention protects copyright by requiring countries to criminalise the intentional infringement of copyright and related rights on a commercial scale by means of a computer system. New Zealand's legislation is already aligned with the copyright-related provisions of the Convention. The Convention does not require New Zealand to accede to any treaties relating to copyright to which New Zealand is not already party.

Human rights and upholding the principles of the Treaty of Waitangi | Te Tiriti o Waitangi

80. The Convention includes provisions that explicitly require enforcement powers and procedures be conducted with respect for fundamental human right and freedoms, such as freedom of expression, protection and privacy of personal data, and non-discrimination.

81. Some Māori we heard from raised a concern that international interests may be put ahead of the Crown's obligations to Māori when considering and responding to mutual assistance/data preservation requests. One of these obligations is that the Crown promises that its obligations to New Zealand citizens are owed equally to Māori.

82. The Convention upholds the rights of countries to protect the rights of its citizens, including by retaining ultimate discretion over whether to assist in mutual assistance requests under grounds set in its own legislation. New Zealand's mutual assistance legislation protects the legal values of natural justice, due process, fairness and equity.

83. Concerns about the impact of the Convention on the Crown's obligations to Māori will continue to be addressed as the Convention is implemented in New Zealand law.

Economic effects

84. Accession is not expected to have a significant impact on New Zealand's economy.

85. A large portion of cybercrime, such as fraud, causes economic loss for businesses, the government, and individuals. Better approaches to addressing cybercrime and other crime would reduce the economic loss. While losses from cybercrime can be difficult to quantify it appears that they are significant:[7]

    a) CERT NZ recorded 4740 cyber security incidents in 2019 with over $16.7 million in financial losses. The most common incidents were phishing and credential harvesting (stealing passwords), scams and frauds, and unauthorised access. A half-year report from 2020 shows that cyber security incidents have increased by 42%, compared to the same time period in 2019.[8]

    b) The Reserve Bank released a report in February 2020 which focused on the cost of cyber incidents in the financial sector. It estimated the average costs of cyber incidents to be around $104 million per annum for the banking industry and $38 million per annum for the insurance industry.[9]

    c) The National Cyber Security Centre recorded 352 cyber security incidents in the 12 months to 30 June 2020.[10]

---

[7] 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.

[8] 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/

[9] Reporting is at https://www.rbnz.govt.nz/research-and-publications/reserve-bank-bulletin/2020/rbb2020-84-02

[10] The National Cyber Security Centre responds to threats to nationally significant organisations and high-impact cyber incidents at the national level. Reporting is at: https://www.ncsc.govt.nz/newsroom/cyber-threat-report-2020/

86. In addition to economic loss, cyber security incidents can have negative impacts for public confidence in computer systems, for example, in relation to conducting business over the internet. This has been highlighted recently, with a global campaign of denial of service (DoS) events affecting a range of New Zealand organisations.

Social effects

87. Cybercrime not only results in financial harms. It can result in physical and mental harms and be frightening to those targeted. Although there is no New Zealand data on the extent of these types of harms, a UK report found that victims of cybercrime reported psychological impacts such as stress (75%) and anxiety (70%), and impacts on physical or mental health such as difficulty sleeping (53%), depression (43%), and stress-related illnesses (42%).[11]

88. In addition, the Ministry of Justice Crime and Victim Safety Survey report from 2019 found that adults with low life satisfaction and a low feeling of safety were significantly more likely to experience fraud and cybercrime incidents.

89. The ability to investigate cybercrime and other crime better would contribute to more effective criminal investigations in New Zealand. This would mean better resolution of criminal cases.

90. Better results for victims would have flow-on effects for another strategic priority of proactively tackling cybercrime: improving the reporting experience for victims and contributing to a culture where cybercrime is reported and resolved. A key area of focus in the 2019 Cyber Security Strategy is “encouraging reporting of cybercrime and improving sharing of information about cybercrimes”.

The costs to New Zealand of compliance with the treaty

Crown

91. Accession would create some ongoing costs associated with servicing international commitments (e.g. reporting on compliance with Convention requirements, and attending T-CY meetings), monitoring and reporting on the implementation of new Search and Surveillance Act powers, as well as operating the 24/7 point of contact function. These costs will be absorbed within existing agency baselines.

Private sector

92. Preservation orders will create a new compliance costs for those required to execute them. The costs will include time and resources spent on receiving and executing the order, and the infrastructure to hold the data. The estimated total cost of compliance for industry will average in the order of $15,000 annually.

[11] Victims of Computer Misuse (2020) Professor Mark Button, Dr Lisa Sugiura, Dean Blackbourn, Dr Richard Kapend, Dr David Shepherd, and Dr Victoria Wang. *University of Portsmouth*.

Completed or proposed consultation with the community and parties interested in the treaty action

Public consultation to date

93. Public consultation was undertaken in July-September 2020. The published consultation paper focused on the proposal that New Zealand accede to the Convention, and the details of a preservation order scheme to be included in the Search and Surveillance Act 2012. In addition to publishing a consultation paper, several virtual meetings were held with stakeholder groups.

94. An information session was held for the telecommunication and data storage sectors to outline the proposed data preservation scheme and provide the opportunity to respond to questions. The telecommunications companies and several other companies with a role in the industry had previously been consulted on a data preservation scheme in early 2019, and their responses had influenced the version that was consulted on in 2020.

95. Drawing on the Te Arawhiti framework for Crown engagement with Māori, and the 2001 Strategy for Engagement with Māori on International Treaties, Māori groups and organisations who might have an interest in the proposals were also consulted. Many of these organisations and individuals had also attended the hui in January 2020.

96. Accession to the Convention was also consulted on as part of the development of the New Zealand Cyber Security Strategy 2019 (and previous strategies in 2011 and 2015). The strategy was consulted with stakeholders from a range of non-government and private sector organisations and the public, and overall, there was clear and strong support for accession.

97. In addition to the consultation undertaken on the data preservation scheme and accession to the Convention, the Law Commission undertook extensive consultation as part of their reviews of the Search and Surveillance Act 2012 (a joint review with the Ministry of Justice), and on mutual assistance and extradition law. This report set out recommendations for a preservation order scheme, which have been the basis for the proposed scheme.

Summary of feedback received in submissions

98. The public consultation period in July-September 2020 resulted in 17 submissions from a range of private sector companies, organisations, and individuals.

99. The majority of submitters supported accession to the Convention. Submitters acknowledged that accession would be a benefit to New Zealand to address international crime, to support international cooperation, and to play an international role in promoting a rules-based order.

100. Many of the submissions focused on the proposed data preservation scheme, and its parameters:

    a) Telecommunications and data storage companies supported the proposed tightly-constrained scheme to limit costs, while other submitters supported a tightly-constrained scheme to limit the impact on digital privacy rights.

    b) Telecommunications companies submitted that the costs of data preservation would be higher than those outlined in the consultation paper and supported a cost

recovery scheme. Data storage providers noted that the costs are likely to be already incorporated into the costs of doing business. This may be due to the different business models of each company, and compliance costs may not be comparable across these businesses.

c) Support was expressed for an appeal mechanism, as well as annual reporting on data preservation orders, safe harbour provisions for companies required to preserve data, and guidance for industry on the new orders.

101. Submitters also addressed the other legislative changes required to implement the Convention:

a) One submitter opposed the proposed changes to the Mutual Assistance in a Criminal Matter Act 1992, as in their view this Act should be reviewed as a whole, rather than progressing small amendments.

b) Further guidance was requested on confidentiality orders, and how they align with existing Privacy Act requirements.

102. Feedback from Māori submitters pertained to the use and protection of Māori data, and fears that international interests may supersede the Crown's obligations under the principles of the Treaty of Waitangi | Te Tiriti o Waitangi. Concern was also expressed that greater international cooperation may exacerbate the overrepresentation of Māori in the criminal justice system. A desire for further consultation and engagement was also expressed.

Response to feedback received in consultation

103. Overall, the support for accession has been positive. Concerns from Māori about Māori data and overrepresentation touch on much wider issues than the subject matter addressed by the Convention, and further dialogue on these topics will be undertaken (see section on cultural effects).

104. The feedback about the parameters of the data preservation scheme, and feedback on the other legislative changes has been incorporated into policy advice to Ministers.

105. There will be further opportunities for public consultation and scrutiny through the Select Committee process. The Select Committee will take public submissions on the specific legislative changes required by the Convention during the passage of implementing legislation.

Consultation across government

106. Crown Law, the Department of Internal Affairs, the Ministry of Business, Innovation and Employment, the Ministry of Foreign Affairs and Trade, the New Zealand Intelligence Community, the New Zealand Police, Stats NZ, Te Arawhiti, Te Puni Kokiri, and the Treasury have been consulted on the implementation of the Convention.

107. The Ministry for Primary Industries, the Ministry of Transport, the New Zealand Customs Service, the Government Chief Privacy Officer, and the Office of the Privacy Commissioner were also consulted on the parameters of the data preservation scheme.

Subsequent Protocols and/or amendments to the treaty and their likely effects

108. 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 any proposed change. After all Parties have accepted the amendment, the Committee of Ministers would adopt these changes and they would come into force.

109. Amendments to the Convention do not automatically apply to Parties. Any future binding treaty actions, including accession to Additional Protocols, would require Cabinet approval, which would be sought at the appropriate time.

110. There is currently one Additional Protocol to the Convention, "concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems." Negotiations between Parties to the Convention are also currently underway on a Second Additional Protocol which covers enhanced international cooperation and access to evidence in the cloud, to help law enforcement secure evidence on servers in foreign, multiple, or unknown jurisdictions. This Protocol would also require separate consultation and Cabinet approval.

Withdrawal or denunciation provision in the treaty

111. As per Article 47, any Party to the Budapest Convention may, at any time, denounce its obligations under the Convention by means of a notification addressed to the Secretary-General of the Council of Europe. This takes effect after three months, and there are no continuing obligations.

Agency Disclosure Statement

112. The Ministry of Justice and the Department of Prime Minister and Cabinet have prepared this National Interest Analysis (NIA) in consultation with other relevant government agencies. This NIA identifies the substantive legal obligations in the Convention that would require legislative implementation and analyses the advantages and disadvantages to New Zealand in becoming a party to the Convention.

113. This NIA identifies costs that some companies who hold data may have to bear. However, these are limited by the implementation of a tightly constrained data preservation scheme, and the very low volume of orders likely to be made annually.

114. Obligations under the Convention would not impair private property rights, market competition, or the incentives on businesses to innovate and invest; or override fundamental common law principles.

Oliver Sanders

Policy Manager, Sentencing and Rehabilitation Policy

Ministry of Justice Date:

_____ _____

Sophie Vickers

Manager, National Cyber Policy Office

Department of the Prime Minister and Cabinet Date:

_____ _____

Adequacy Statement

The Ministry of Justice confirms that this National Interest Analysis is adequate and that the principles of the Government Expectations for Good Regulatory Practice and the regulatory impact analysis requirements have been complied with.