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

6 November 2023

[redacted]

Ref: OIA-2023/24-0224

Dear [redacted]

**Official Information Act request relating to the May 2023 interim report of the Encryption Working Group**

Thank you for your Official Information Act 1982 (the Act) request received on 5 October 2023. You requested:

> *"I am a New Zealand citizen writing with an OIA request, please.*
>
> *Specifically, please provide me with the May 2023 interim report of the Encryption Working Group referred to at [28](a) of your Cyber Security Strategy Annual Report 2022/23 (20 September 2023). https://www.dpmc.govt.nz/sites/default/files/2023-09/cyber-security-strategy-annual-report-2022-23.pdf*
>
> *Apologies for the request if there is already a copy online—I couldn't locate one but am conscious another agency may have uploaded it."*

Please find a copy of the May 2023 interim report of the Encryption Working Group attached as requested. I have decided to release this document to you subject to information being withheld as noted. The relevant grounds under which information has been withheld are:

- section 6(a), to protect the security or defence of New Zealand or the international relations of the Government of New Zealand
- section 6(b)(i), to protect the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government
- section 6(c), as the making available of this information would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial
- section 9(2)(b)(i), to prevent disclosure of a trade secret
- section 9(2)(f)(iv), to maintain the confidentiality of advice tendered by or to Ministers and officials
- section 9(2)(g)(i), to maintain the effective conduct of public affairs through the free and frank expression of opinion.

Where information has been withheld under section 9 of the Act, in making my decision, I have considered the public interest considerations in section 9(1) of the Act. No public interest has been identified that would be sufficient to override the reasons for withholding that information.

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on the Department of the Prime Minister and Cabinet's website during our regular publication cycle. Typically, information is released monthly, or as


Executive Wing, Parliament Buildings, Wellington, New Zealand 6011
☎ 64 4 817 9698 www.dpmc.govt.nz

otherwise determined. Your personal information including name and contact details will be removed for publication.

Yours sincerely

Julian Grey
**Acting Deputy Chief Executive**
**National Security Group**

# ENCRYPTION WORKING GROUP PRELIMINARY REPORT

## Introduction

1. Encryption provides economic value and utility to governments, the private sector, and end-users alike. It delivers critical privacy and cyber security controls that support the vision of a resilient and future-focused economy, as outlined in the Digital Strategy for Aotearoa.
2. The importance of encryption in protecting human rights is exemplified in repressive states, where end-to-end encrypted (E2EE) messaging apps allow human rights defenders to seek, receive and impart information securely and associate online.
3. The inherent value of privacy has also led globally to demand-driven reasons for the provision of privacy that E2EE offers. As the tech sector expands, market trends have led to consumers and businesses preferring strong encryption for their digital products and services. As of 2022, 50% of private companies across all business sectors were using encrypted solutions.[1]
4. Service providers across the wider technology industry now deliver a wide range of products and services with strong encryption as a core part of their offering. In an indication of the global popularity of E2EE applications, four of the six most-used messaging apps globally offer E2EE as a default or opt-in.[2]
5. …But E2EE also creates two distinct problems for law enforcement, national security and public safety:
    a. E2EE enables criminal offending by shielding from investigators unlawful content data,[3] incriminating communications between suspects and the identification of offenders/people involved in these communications. For example, without the ability to examine content data suspected to contain child sexual abuse material (CSAM) or terrorist and violent extremist content (TVEC), investigators will be unable to determine if any images or videos are objectionable material contrary to the Films, Videos and Publications Classifications Act 1993.
    b. E2EE can make it more difficult for service providers to identify and manage harmful and illegal content (such as CSAM or TVEC) on their services, which makes it much harder to prevent, and report criminal activity on their networks.
6. However, there is a lack of data to weigh up the impact of E2EE on law enforcement and public safety against the broader privacy, human rights, security, and economic benefits.



[1] Encryption Consulting Study on Global Encryption Trends – 2023 - Global average adoption of enterprise encryption strategy is 50% https://www.encryptionconsulting.com/global-encryption-trends-2023/#downloadReport
[2] Tech Against Terrorism, Terrorist Use Of E2EE Report, page 5
[3] Content data includes the text, audio file, video file, photo or other image

7. In February 2022 the Cyber Security Strategy Coordination Committee (CSSCC) agreed to the following work programme:

    a. Collection of relevant data to inform recommendations in a report to the CSSCC on how law enforcement can access the information it needs from E2EE applications while protecting the rights of New Zealanders to privacy and security.

    b. Establishment of a cross-agency working group, the Encryption Working Group (EWG) to interpret the data and draft a report to the CSSCC to highlight areas of common interest, gaps or inconsistencies, or areas where a common approach across different regulatory systems might be valuable to achieve government objectives.

8. In May 2022 Ministers[4] endorsed this Work Programme to enable decision makers to understand the impact of E2EE on investigations and public safety.

9. The EWG members (see Annex A) agreed a project plan (Annex B) to interpret the data collected to inform recommendations in a draft Report.

10. The EWG met in-person in September, October and December in 2022 and in February in 2023 and have continued to collaborate virtually to present this Preliminary Report with recommendations informed from the available data, open source resources, international engagement with like-minded partners and meetings with technology companies.

11. It is important to note that this Report **does not** provide detailed comment on the benefit of E2EE in a New Zealand context, and there is a need to consider the commissioning of research on how law enforcement solutions might undermine New Zealand's broader economic goals, human rights, and any unintended consequences of enabling lawful access. As this broader research and analysis is yet to be completed, this Report can only be viewed as preliminary.

12. As per the project plan, the CSSCC is invited to consider if this Preliminary Report should be peer reviewed by independent Crown Entities, academics, the private sector, non-governmental organisations, civil society and community groups.

13. Should the CSSCC direct a peer review, the EWG will review responses from the peer reviewers before submitting a final Report to the CSSCC by September 2023.



[4] Former Minister of National Security and Intelligence (Rt Hon Jacinda Ardern), Minister Responsible for the NZSIS and GCSB (Hon Andrew Little), Minister of Internal Affairs (Hon Jan Tinetti), Minister of Justice (Hon Kiri Allan), Former Minister for Police (Rt Hon Chris Hipkins) and Former Minister for Customs (Hon Meka Whaitiri)

## Abbreviations

| | |
|---|---|
| ACIC | Australian Criminal Intelligence Commission |
| AFP | Australian Federal Police |
| CMC | Crime Monitoring Centre |
| CSAM | Child Sexual Abuse Material |
| CSSCC | Cyber Security Strategy Coordination Committee |
| DECD | Dedicated Encryption Communication Device |
| DFU | Digital Forensic Unit |
| E2EE | End-to-end Encryption |
| FB | Facebook |
| IGIS | Inspector-General of Intelligence and Security |
| IPCA | Independent Police Conduct Authority |
| ISA | Intelligence and Security Act 2017 |
| NCMEC | National Center for Missing and Exploited Children |
| NSIP | National Security Intelligence Priorities |
| OPC | Office of the Privacy Commissioner |
| OTT | Over-The-Top |
| SLAID | Surveillance Legislation Amendment (Identify and Disrupt) Act 2012 |
| SSA | Search and Surveillance Act 2012 |
| UK | United Kingdom |
| US | United States of America |
| TICSA | Telecommunications (Interception Capability and Security) Act 2013 |
| TNOC | Transnational Organised Crime |
| TVEC | Terrorist and violent extremist content |
| VoIP | Voice over Internet Protocol |
| VPN | Virtual Private Network |

## Executive Summary

1. The EWG presents the recommendations in this Preliminary Report to the CSSCC after nine months of analysing available data, engaging with international partners and consulting with stakeholders.[5] The Preliminary Report predominately focuses on the difficulties law enforcement agencies face when it comes to E2EE, the lack of informative data and recommends further policy analysis to fully understand the issues in the New Zealand context.

2. Implementing the following recommendations may require greater resourcing than is currently available from the EWG and reprioritising resources from elsewhere. Further, analysis on the benefit of E2EE may need to be done by an external consultant, due to the lack of current expertise within agencies.

3. The EWG has been unable to collect sufficient data from agencies to inform the impact of E2EE and encrypted communications on public safety. To leverage other opportunities to collect data, the EWG identified an activity in the Year Four (2023) TNOC Strategy Action Plan 6(c) . The **first recommendation**, therefore, is for the Year Four (2023) TNOC Strategy Action Plan to collect sufficient data 6(c)

4. s9(2)(f)(iv)

5.

6.

[5] As the Chair, DPMC has engaged with NetSafe and the Office of the Privacy Commissioner and Michael Dizon presented to the EWG in December 2022.
[6] See paragraph 56 and *Figure 5* in Recommendation One
s6(c)
[8] 2022 periodic review of the Intelligence and Security Act 2017: Terms of Reference | New Zealand Ministry of Justice

7. s9(2)(f)(iv) 

8. It is also important to note New Zealand's policy development on E2EE cannot happen in isolation from overseas developments. The EWG is aware of the need to monitor these international developments, especially when it comes to jurisdictional issues and companies potentially withdrawing from markets where law enforcement access to information undermines the confidentiality and integrity of its product. Further, there are significant challenges in imposing domestic law on service providers that have no or little physical presence in New Zealand (i.e. New Zealand regulation and court judgements are generally not enforceable on foreign entities).

9. These issues are only likely to intensify as the range of applications offered by service providers outside of New Zealand that use E2EE multiply, and suggest that multilateral approaches to these issues are likely to prove more fruitful than unilateral domestic law changes. Exceptional lawful access[14] for E2EE service providers is a focus of a Five Country working group. The **fourth recommendation**, therefore, is for DPMC to coordinate any agreed next steps following presentation and agreement by New Zealand of the working group proposals to the Five Country Ministerial in June 2023.



[9] Recommendation 46 of the Law Commission Review of the Search and Surveillance Act 2012, June 2017, Report 141 [hereinafter NZLC R141]
[10] Ibid., Recommendation 47
[11] 9(2)(f)(iv)
[13] The Legislation Design and Advisory Committee guidelines also outline domestic considerations for sentence increases: http://www.ldac.org.nz/assets/documents/LDAC-Legislation-Guidelines-2021-edition.pdf
[14] "Exceptional lawful access" means a targeted government authorization to access data belonging to a user as part of a law enforcement or national security investigation, with the assistance of a service provider. The access is exceptional because it will not affect the cybersecurity of legitimate users and not diminish the quality of service provided.

**Recommendation ONE: NZ Police** to establish an evidence base 6(c)

**Recommendation TWO:** s9(2)(f)(iv)

**Recommendation THREE:** s9(2)(f)(iv)

**Recommendation FOUR: DPMC** to lead agency coordination on any next steps following the Five Country working group proposals on exceptional lawful access to the Ministerial in June 2023

## Methodology

EWG mapping of relevant workstreams

1. As a preliminary step, to prevent duplication of resources and leverage any opportunities, a mapping exercise was completed to confirm if any other policy workstreams were analysing the impact of encryption on law enforcement investigations.[15]

2. The other workstreams considered were:

    a. the Transnational Organised Crime (TNOC) Strategy

    b. Intelligence and Security Act 2017 Review

    c. Search and Surveillance Act 2012 Review (presently paused)

    d. Royal Commission of Inquiry into the terrorist attack on Christchurch Masjidain recommendations

    e. Cloud First Policy Refresh

    f. Christchurch Call

    g. Police led Cybercrime Risk Landscape Analysis

    h. Digital Strategy for Aotearoa

    i. Royal United Services Institute horizon-scanning of existing and emerging technologies

    j. Emerging Technology Policy Working Group.

3. The mapping concluded that none of the above work programmes were considering the benefit of E2EE providers to the New Zealand public, businesses and potential unintended consequences exceptional lawful access may create. Furthermore, to date there has been limited analysis done on the interaction between law enforcement access to E2EE data and Māori views and perspectives.

4. Of the workstreams mapped, of most relevance is the Year Four TNOC Strategy, 6(c) [redacted]

5. The EWG concluded the potential cross-over between the E2EE Work Programme and the TNOC Strategy 6(c) [redacted] (see **Recommendation One**).

[15] See the table in Annex C of workstreams connected to the E2EE Work Programme

EWG data collection

6. At the commencement of the work programme, DPMC requested agencies to confirm the data they held to show the impact of E2EE on their investigations. The intention was for this data to inform recommendations on how agencies can access the information they need to ensure New Zealanders are protected from harm, while also protecting individual rights to privacy and security.

EWG papers

7. Alongside this data collection, DPMC drafted an Issues Paper (Annex D) with specific questions for agencies to consider to support the development of recommendations based on the data collected.

8. EWG members were tasked to propose recommendations that addressed the questions in the Issues Paper. Another challenge that was identified from these EWG proposals, was access to encrypted devices equally hampered investigations. For this reason, the EWG agreed that any recommendations should consider both encrypted devices and E2EE.

9. The EWG assessed each proposed recommendation as follows:

    a. **High Priority:** Benefits of reducing the risk of harm to the public outweigh costs
    b. **Medium Priority:** The recommendation has balancing costs and benefits
    c. **Low Priority:** The cost of the recommendation outweighs the benefits

Preliminary Report outline

10. This Preliminary Report includes the recommendations the EWG assessed as **High Priority** and analyses each using the following headings:

    a. Summary of the recommendation;
    b. How the recommendation will protect the public from harm;
    c. Impact of the recommendation on the following:
        i. Human rights of targeted individuals and others;
        ii. Crown's responsibilities to Māori underneath Te Tiriti o Waitangi (preliminary analysis);
        iii. Commerce, economic competitiveness and innovation (preliminary analysis);
        iv. International relationships; and
        v. Overall security of New Zealand (preventing interventions that weaken cyber security)

11. The Preliminary Report has been divided into the following sections, with a problem definition for each section, and the proposed next steps:

**a. Collection of Data**

**Recommendation ONE: NZ Police** to establish an evidence base 6(c)

**b. Legislative review**

**Recommendation TWO:** s9(2)(f)(iv)

**Recommendation THREE**: s9(2)(f)(iv)

**Recommendation FOUR: DPMC** to lead agency coordination on any next steps following the Five Country working group proposals on exceptional lawful access to the Ministerial in June 2023

## Data Collection

**PROBLEM:** *Insufficient New Zealand specific data on the impact of encryption on criminal investigations and public safety.to inform allocation of resources and training needs*

**Recommendation ONE: NZ Police** to establish an evidence base 6(c)

**Next steps:**

- Dedicated resource funded through the TNOC Strategy
- Timeframe: data collection Q1 2023/24, reporting Q2 2023/24

**Summary**

NZ Police unable to provide data of the full extent of the criminal use of E2EE

1. 6(c)
2. 6(c)
3. 6(c)
4. The following sections of this Report highlight available data provided by NZ Police and reference the EWG recommendation that further data should be collected 6(c)

Criminal justice outcomes decrease and cybercrime reports increase

5. Since NZ Police started recording the online environment as a crime scene, there has been a noticeable decline in case resolutions (i.e. charge/prosecution or pre-court disposal) due to their being no further lines of inquiry (*Figure 1*).

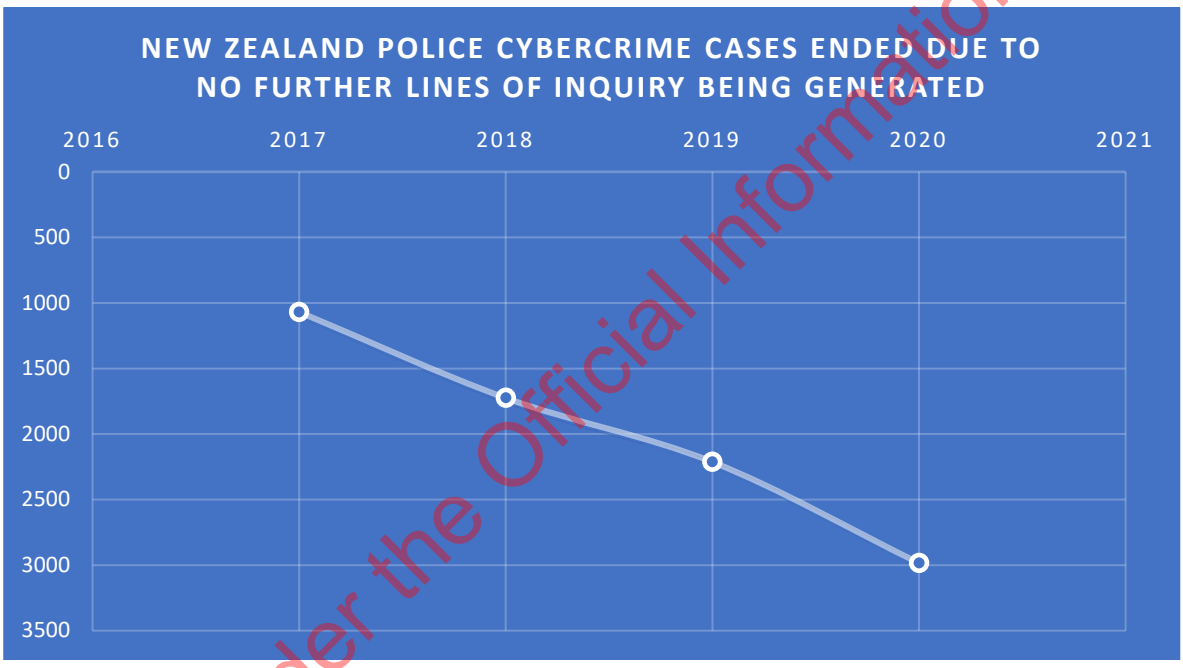
[16] 6(c)

6. This is despite a 45% increase in cybercrime[18] reported to New Zealand agencies between 2019 and 2022. A joint 2022 National Centre for Cyber Security and NZ Police assessment concludes, that given international trends, cybercrime in New Zealand has actually risen by approximately 80% since 2019.[19]

7. Online Fraud and cybercrime represented the greatest proportion of victimised adults in the previous 12 months[20] and direct financial losses to New Zealand from cybercrime is likely to be over $1b annually and increasing (these estimates do not include response and recovery costs).[21]

8. Resource constraints, evidence collection from other jurisdictions and offenders located outside of New Zealand have impacted case resolutions. 6(c)

***Figure 1***




Interception data

9. The NZ Police Crime Monitoring Centre (CMC) facilitates and monitors lawful interception of electronic communications in support of serious crime investigations.

10. 6(c)

[18] The Joint Cyber Intelligence Report, New Zealand's Cyber Crime Landscape, CIR-2022-893, 30 November 2022 at page 2 defines cybercrime as cyber-enabled crime such as fraud, online harm and cyber security incidents (which the report states '99% are criminal in nature)"

[19] Joint Cyber Intelligence Report, New Zealand's Cyber Crime Landscape, CIR-2022-893, 30 November 2022

[20] According to the New Zealand Crime and Victim Survey, cybercrime and fraud has become New Zealand's most populous crime type with 8% of adults (approx. 318,000 adults) being a victim of cybercrime and fraud over the 12 month reporting period (https://www.justice.govt.nz/assets/Documents/Publications/Cycle-4-Core-Report-v0.20-20220628.pdf).

[21] Joint Cyber Intelligence Report, New Zealand's Cyber Crime Landscape, CIR-2022-893, 30 November 2022

11. 6(c)

12. CMC has observed increasing migration from, predominantly telephony and SMS electronic communications, to mobile data enabled Over-the-Top (OTT) messaging applications s6(c)

***Figure 2***

6(c)

13. 6(c)

***Figure 3***

6(c)

[22] 6(c)

14. 6(c) [redacted]

15. 6(c) [redacted]

**EWG conclusion on CMC data**

16. The CMC data only confirms how often E2EE OTTs are referred to in interception operations and does not resolve the problem definition of having sufficient data on the impact of encryption on criminal investigations and public safety to inform allocation of resources.

17. 6(c) [redacted]

18. 6(c) [redacted]

19. 6(c) [redacted]

    a. 6(c) [redacted]

    b. 6(c) [redacted]

20. 6(c) [redacted]

21. On the basis the data is available and requires resourcing to collate, the EWG support this data collection is resourced as part of the Year Four (2023) TNOC Strategy Action Plan.

22. This data collection also complements the National Security and Intelligence Priorities (NSIPs) to support agencies to detect serious crime, trends and enablers that make transnational crime more efficient, effective, undetectable or disguisable.[25]

<u>Unexaminable devices</u>

23. Following the EWG conclusions on the CMC data, NZ Police provided information about devices designated as unexaminable, based on data from NZ Police's High Tech Crime Group record management systems and databases. The information provided was collected from live databases, therefore, is approximate and subject to change.

[25] https://www.dpmc.govt.nz/our-programmes/national-security/national-security-intelligence-priorities

24. 6(c) [redacted]

25. 6(c) [redacted]

***Figure 4***

6(c) [redacted]

26. 6(c) [redacted]

27. 6(c) [redacted]

28. 6(c) [redacted]

29. 6(c) [redacted]

30. 6(c) [redacted]

31. 6(c) [redacted]

32. 6(c) [redacted]

**EWG conclusion on data on unexaminable devices**

33. To determine what resources are necessary it is important to know for the devices that were unexaminable 6(c) [redacted] :

    a. A breakdown of the crimes investigated;
    b. How many investigations were stopped due to the devices being unexaminable;
    c. Breakdown of the specific crimes being investigated that were stopped due to devices being unexaminable;
    d. Of those investigations that proceeded despite exhibits being unexaminable were Police NZ – on the basis of other supporting evidence – still able to:
        i. Charge?
        ii. Secure a conviction?
    e. How many unexaminable devices were retained/returned?

34. The additional data requested will allow NZ Police to understand:

    a. The impact on investigations of unexaminable devices (i.e. did Police NZ continue the investigation despite devices being unexaminable and did this lead to a successful outcome?);
    b. The risk of harm caused by unexaminable devices (i.e. where investigations had commenced what offences could not be investigated due to the devices being unexaminable?); and
    c. Possible solutions based on this data (i.e. does the data support an increase in specific tools to access devices, use of more commercial off the shelf tools, more personnel and investment in training?).

35. 6(c) [redacted] the EWG support data being collected on the impact of unexaminable devices on investigations to inform where resources, both technical and personnel, need to be allocated to protect New Zealanders from harm.

36. This data collection again complements the transnational serious and organised crime NSIP to support agencies to detect serious crime enablers.

Dedicated Encrypted Communications Devices

37. A Dedicated Encrypted Communication Device (DECD) is a modified mobile phone with bespoke applications to ensure communications between handset owners can occur securely and anonymously.[26] DECDs cost approx. $2,000 to purchase and six month subscriptions are an additional $2,000, meaning a device can cost $4,000 - $6,000 per year.

38. 6(c)

39. 6(c)

40. 6(c)

6(c)

6(c)

41. Infiltrating DECDs through traditional law enforcement methods (i.e. search warrants and telecommunications interception) has proved largely ineffective, due to sophisticated security mechanisms, that prevent identifying users or where they are being used. When lawful interception is attempted, very little useable data is able to be received by law enforcement.[27]

42. Despite this, there have been some notable successes, where law enforcement have been able to cooperate with other jurisdictions who have shared intelligence leads after using their different legal settings to access seized DECDs. These different legal settings enable law enforcement to access communications before they are encrypted.

[26] Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 Submission 6 - Supplementary Submission by the Australian Federal Police, April 2021, page 4
[27] Ibid., page 4

43. The sharing of intelligence by these jurisdictions, has led to the prevention and detection of serious crimes across the world, that would otherwise have remained undetected. Examples of these successes include EncroChat and Anøm

*EncroChat*[28]

44. French authorities first detected the use of EncroChat services in 2017. By early 2020, EncroChat had 60,000 users engaged in criminal activity. Law enforcement frequently seized these devices as evidence in investigations, but standard forensic extraction devices were not able to overcome EncroChat's encryption measures.

45. Eventually, it was possible for French authorities, based on French legal provisions,[29] and following research and development efforts to circumvent EncroChat's encryption, to obtain access to the users' communications.

46. Law enforcement monitored and analysed EncroChat communications in real time during a three month period. Over 100 million intercepted text messages exchanged by tens of thousands of users, mostly based in Europe, triggered a significant number of investigations mostly concerning drugs trafficking and connected criminal activities such as violent crimes, money laundering and corruption.[30]


*Images of controlled drugs, money and a torture chamber shared by EncroChat users and the message shared by the EncroChat provider after the Police accessed communications*

[28] Adapted from the Europol and Eurojust Third Report of the Observatory Function on Encryption 2021

[29] In France, law enforcement in the EncroChat investigation used Articles 230-2 and 706-102-1 of the Code of Criminal Procedure, to install technical tools to capture encrypted data and to decrypt the content of seized devices.

[30] Images openly shared by offenders in Europe discussing their criminal behaviour across the EncroChat platform, including drugs, money and a shipping container equipped as a torture chamber. EncroChat also advised platform users that their system had been compromised and how to avoid detection. Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe | Europol (europa.eu) and the Australian Parliamentary Joint Committee on Intelligence and Security - Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 – February 2021 Submission by the Australian Federal Police

*Operation Trojan Shield*

47. During Operation TROJAN SHIELD, the FBI successfully created a DECD called Anøm, the sole purpose of which was to facilitate secure communications between criminals.[31] The New Zealand operation after the US shared intelligence was code named Operation SPYGLASS.

48. 6(c) [redacted]

49. 6(c) [redacted]

**EWG conclusion on use of DECDs**

50. Whilst the use of DECDs has been limited in New Zealand, the results from intelligence and evidence shared from law enforcements agencies outside New Zealand, has been integral to successful criminal justice outcomes in New Zealand. As TNOC groups purchased DECDs on the basis they believed their communications could not be accessed, when law enforcement do access, there is a vast array of incriminating evidence against criminal networks.

51. As most significant DECD intelligence leads have been from Europe, the Europol data sharing agreement[32] with New Zealand will be an important mechanism to share future information to proactively investigate those TNOC groups who use DECDs in New Zealand. However this does not address New Zealand's legal settings that inhibit law enforcement gathering intelligence and evidence

52. As DECDs are only used for criminal purposes, it is important that New Zealand has regulatory settings that are fit for purpose to enable access in New Zealand, rather than relying upon intelligence and evidence from other jurisdictions. s9(2)(f)(iv) [redacted]

53. If more data is collected on the scale and impact of DECDs in New Zealand as part of the Year Four (2023) TNOC Strategy Action Plan, this may support the commencement of policy analysis to prohibit the possession and supply of DECDs. New South Wales passed legislation in October 2022 establishing a scheme for DECD prohibition orders (Dedicated Encrypted Criminal Communication Device Prohibition Orders Bill 2022)[33] and the UK Home

[31] Europol (2021, 8 June). *800 Criminals Arrested in Biggest Ever Law Enforcement Operation Against Encrypted Communication*. Retrieved from: www.europol.europa.eu.

[32] "Agreement between the European Union (EU), of the one part, and New Zealand, of the other part, on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the authorities of New Zealand competent for fighting serious crimes and terrorism" (the Agreement) will enhance cross-border information sharing between New Zealand and the EU for preventing and responding to serious crimes and terrorism.

[33] https://www.parliament.nsw.gov.au/bills/Pages/bill-details.aspx?pk=4006

Office recently consulted (January-March 2023) on legislative proposals[34] to improve law enforcement responses to serious organised crime, specifically offences for supplying and possessing DECDs.

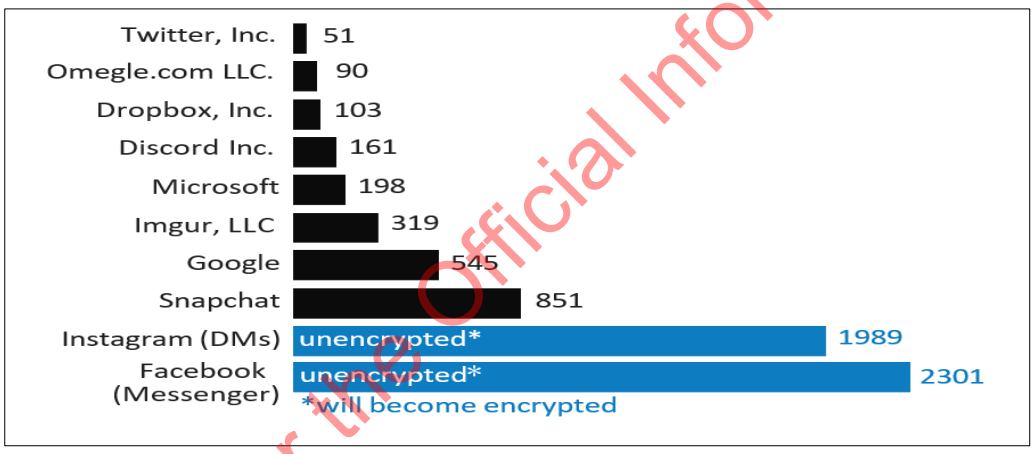
Impact of E2EE on objectionable material investigations

54. The DIA's Digital Safety Team, NZ Customs and NZ Police receive CSAM CyberTips[35] from the National Center for Missing and Exploited Children (NCMEC). The immediate impact of E2EE on these investigations is the inability of technology companies to provide CyberTips to NCMEC on the basis they are unable to scan across their platforms for CSAM content.

55. Currently, four of the top ten companies that send CSAM CyberTips[36] to NCMEC use E2EE for private messages on their platforms: Meta (WhatsApp), Google, Snap and Skype.

56. Meta's 'Privacy First' proposal is of immediate concern because the vast majority of the referrals of CSAM come from Meta (27.1 million out of a total of 31.8 million reports in 2022), whose FB Messenger and Instagram Direct Messages are intended to be E2EE by default in 2023.[37] *Figure 5* confirms the majority of the 2021/22 referrals of reported online CSAM to New Zealand, were from Meta platforms (Facebook Messenger and Instagram).

***Figure 5***




57. If Meta implements E2EE by default, it will be unable to detect CSAM images on its platforms by means of its current photo-matching technology, that generates most of its CyberTips. This means that law enforcement will receive far fewer CyberTips and will rely heavily on user generated CyberTips.

58. However, of equal concern is the fact that many companies under-report or through design cannot identify CSAM. For example, Apple made only 160 referrals in 2021, yet has more than 1.65 billion active devices, all of which have encryption features to safeguard user data.

59. The implication of service providers not maintaining access to content, is not only the likely diversion solely to user reporting, but also the downstream effects of a dearth of reporting

[34] Strengthening the law enforcement response to serious and organised crime - GOV.UK (www.gov.uk)
[35] Service providers in the US are mandated in law to disclose any child sexual abuse material to the National Center for Missing and Exploited Children (NCMEC) – who then disseminate to relevant law enforcement to investigate
[36] Service providers in the US are mandated in law to disclose any child sexual abuse material to NCMEC – who then disseminate to relevant law enforcement to investigate
[37] Testing End-to-End Encrypted Backups and More on Messenger | Meta (fb.com)

and client side understandings and insights. With reduced reporting of harms, the DIA's Digital Safety Group will have restricted ability to take down objectionable material through its Digital Child Exploitation Filter System, and investigate the propagators and instigators of such material. This spans child sexual exploitation and violent extremist and terrorist content, manifestos and associated acceleration of such content and intent online.

**EWG conclusions on impact of E2EE on objectionable material investigations**

60. Maintaining lawful access to communications-related data and content, is crucial to the detection, investigation, and prosecution of objectionable material offences. Technological developments that hinder this access can have a detrimental impact on New Zealand's ability to protect the online safety of our residents.

61. s9(2)(f)(iv) [redacted]

**How the recommendation will protect the public from harm**

62. Collection of more complete data will support NZ Police to support the proposed Year Four (2023) TNOC Strategy 6(c) [redacted]

**Human rights of targeted individuals and others**

63. The data to be collected will be in accordance with existing lawful powers. As such, there is a minimal direct impact on the human rights of individuals.

64. The collection of data will enable policy to be well-designed to ensure it appropriately protects the rights of individuals, including their right to privacy, while providing appropriate tools for law enforcement to protect people from harm.

**Te Tiriti o Waitangi**

65. By nature of the Crown-Māori partnership under Te Tiriti, Māori have tino rangatiratanga over all of their taonga. This includes intellectual property rights which can be protected through E2EE. There can also be taonga in data itself, and so there are particular rights to data sovereignty.

66. Additionally, Māori are disproportionately represented in the criminal justice system. As such, their data is likely to be disproportionately captured by changes to police practices.

67. Officials should take this into account in designing procedures to ensure that data is not improperly captured, held or accessed.

**Commerce, economic competitiveness and innovation**

68. Collecting data can assist policy analysts to develop policies that will not stifle economic competitiveness and encourage innovation.

**International relationships**

69. The collected data, subject to agreement and compliance with the Privacy Act 2020, could assist other jurisdictions to understand the impact of E2EE and encrypted devices on law enforcement investigations.

**Overall security of New Zealand**

70. Collecting data enables policy analysts to consider options to equip law enforcement with appropriate tools without impacting cybersecurity.

## Legislative Review

s9(2)(f)(iv) [Following 9 pages withheld in full under s9(2)(f)(iv)]

**Recommendation FOUR: DPMC** to lead agency coordination on any next steps following the Five Country working group proposals on lawful exceptional access to the Ministerial in June 2023

**Next steps:**

- The CSSCC decides how to collectively resource any required policy analysis.
- The EWG assess that 2 FTE will be required – with DPMC coordinating cross-agency policy analysis and any international engagement

**Summary**

1. The E2EE work programme agreed by the CSSCC highlighted that the overarching encryption environment will be strongly influenced by international technology, market and regulatory developments.[61]
2. This requires an ongoing effort to monitor and influence international activity, including engagement with close security partners at the Five Country senior officials' group on countering online Child Sexual Exploitation and Abuse, and E2EE.
3. s6(a)
4. s6(b)(i)
5. s6(a)
6. s9(2)(f)(iv)
7. 

**Data to confirm why the current situation does not adequately protect the public from harm**

8. Whilst there is no specific data, officials in the EWG have observed that technology companies are increasingly using obfuscating technologies, such as E2EE, that impacts law

[61] Work Programme Proposal on End-To-End Encryption, page 12
[62] s6(a)
[63] s9(2)(b)(i)

enforcement to investigate the most serious crimes (e.g. Meta's Privacy First Policy and introduction of E2EE by default in 2023). As companies race to compete to introduce new private and secure communications, law enforcement access to data to protect people from harm is being increasingly hampered.

9. This is supported by Apple's recent introduction of Advanced Data Protection, s6(b)(i) [redacted]

**How the recommendation will protect the public from harm**

10. The overwhelming majority of digital communication services used by New Zealanders are based offshore. This extra-territoriality issue means that the effectiveness of domestic regulation is significantly affected by regulatory regimes in major markets. New Zealand is unlikely to be able to unilaterally address any issues with exceptional access and safety by design. s9(2)(g)(i) [redacted]

11. The UK passed their Investigatory Powers Act (IPA) in 2016, which includes an effective obligation on technology companies to remove encryption or 'electronic protections' on communications for investigatory purposes after service of a technical capability notice.[65]

12. s6(b)(i) [redacted]

13. [redacted]

14. The Telecommunications (Interception Capability and Security) Act 2013 (TICSA), broke new ground in providing that service providers that provided communications services could be required to comply with domestic interception capability obligations, including the duty to assist with decryption where the provider holds the key.[67]

15. However, TICSA, cannot be used to enforce on overseas service providers offering over-the-top services (such as WhatsApp, Telegram and Signal) to comply with the same intercept capability obligations as domestic service providers.

16. s9(2)(f)(iv) [redacted]

s6(b)(i) [redacted]

[65] See section 253(5)(c) of the Investigatory Powers Act https://www.legislation.gov.uk/ukpga/2016/25/section/253 and The Investigatory Powers (Technical Capability) Regulations 2018, explanatory note, https://www.legislation.gov.uk/ukdsi/2018/9780111163610#:~:text=A%20technical%20capability%20notice%20imposes,the%20obtaining%20of%20communications%20data.

s6(b)(i) [redacted]

the lawful interception of telecommunications under an interception warrant or any other lawful interception authority

s9(2)(f)(iv)

**Human rights of targeted individuals and others**

17. Any exceptional lawful access must not violate or abuse the right to be free from arbitrary or unlawful interference with one's privacy, as set out in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

18. Sufficient safeguards, transparency, accountability and oversight must be considered for any regulatory reform.

19. To understand the privacy implications and alignment of the Privacy Act 2020 in a New Zealand context, the OPC should be consulted as part of any policy analysis.

20. Engagement is also encouraged with other relevant stakeholders, such as NetSafe and InternetNZ, to provide a cross-section of expertise on the human rights implications of any exceptional lawful access proposals.

**Te Tiriti o Waitangi**

21. Consideration in further policy analysis must ensure that any proposed solutions do not disproportionately target Māori or Māori data.

22. Any policy analysis must, therefore, include consultation with Māori to ensure there are appropriate safeguards.

**Commerce, economic competitiveness and innovation**

23. The EWG recognises there is a need to consider alongside the benefits of E2EE, any potential unintended consequences of exceptional lawful access. There are examples from other jurisdictions where service providers are threatening to remove their platforms should they be forced to decrypt user data. For example, Signal[68] and WhatsApp[69] indicated they may stop services in the UK if the government proceeds with its Online Safety Bill requiring Over The Top E2EE services to screen for objectionable content.

**International relationships**

24. Collaborating with our like-minded partners demonstrates our commitment to the *International Statement: End-to-End Encryption and Public Safety* and to enhance information and intelligence sharing and increase cooperation for law enforcement agencies.

25. Engagement that influences development of policy must also be consistent with the Cyber Security International Engagement Plan (March 2021) and the Cyber Security Strategy

[68] Signal says it will shut down in UK if Online Safety Bill approved, The Register, 25 February 2023 https://www.theregister.com/2023/02/25/signal_uk_online_safety_bill/

[69] WhatsApp: Rather be blocked in UK than weaken security, BBC News, 8 March 2023 https://www.bbc.co.uk/news/technology-64863448

priority focus to build international partnerships and cooperation at policy and operational levels.

**Overall security of New Zealand**

26. Any exceptional lawful access must not affect the cybersecurity of legitimate users nor diminish the quality of the service provided.

| Annex: | Classification: | Title: |
|---|---|---|
| **Annex A:** | ~~RESTRICTED~~ | EWG Members |
| **Annex B:** | ~~RESTRICTED~~ | EWG Project Plan |
| **Annex C:** | ~~RESTRICTED~~ | Mapping of Workstreams |
| **Annex D:** | ~~RESTRICTED~~ | EWG Issues Paper |
| **Annex E:** | ~~RESTRICTED~~ | s6(c) |

ANNEXES C, D and E are withheld in full under section 6(c)

# ENCRYPTION WORKING GROUP PRELIMINARY REPORT

## Annexes

**ANNEX A**

**EWG Members**

Ministry of Business, Innovation and Employment

Ministry of Justice

NZ Police

NZ Customs

Joint Directors General Office

Department of Internal Affairs

New Zealand Defence Force

Department of the Prime Minister and Cabinet

## ANNEX B

## EWG Project Plan

### Problem

1. Limited New Zealand specific data on the impact of encryption on criminal investigations and public safety.

### Objective

2. Data collection to inform recommendations on how agencies can access the information they need to ensure New Zealanders are protected from harm, while also protecting individual rights to privacy and security.

### Mandate

3. The Cyber Security Strategy Coordination Committee (CSSCC) agreed and Ministers endorsed a Work Programme for the collection of comprehensive data to enable decision makers to understand the impact of encryption on investigations and public safety.

### Working Group

4. A cross-agency working group, the Encryption Working Group (EWG), will be established to agree:

    a. The data to be collected;

    b. Methodology for data collection to ensure reliability and integrity;

    c. Timeframes for collection;

    d. Ensuring the data collection complies with any confidentiality and privacy obligations.

5. After implementation of the data collection, the EWG will meet monthly to monitor progress and as necessary to respond to any challenges to efficient and effective data collection.

6. Representatives of the following agencies will be invited to the EWG:

    a. CERT NZ

    b. Crown Law

    c. Customs

    d. DIA

    e. DPMC

    f. MBIE

    g. MOJ

    h. GCSB

    i. NZDF

    j. NZSIS

    k. Police

    l. Stats NZ (observer)

m. IRD (observer)

**Governance**

7. The EWG will report to the CSSCC on the progress of the data collection and any issues that affect delivery of the Work Programme.

8. The CSSCC can provide leadership, direction, and coordination at senior levels on delivery of the Work Programme.

**Outcome**

9. The EWG will review and interpret the data collected to inform recommendations in a draft report on how agencies can access the information they need to ensure New Zealanders are protected from harm, taking into account the following:

    a. The ongoing development of encryption technology and existing capabilities to manage the use of end-to-end encryption by malicious actors.

    b. Exploring solutions for access through a variety of investigatory techniques.

    c. International engagement with like-minded jurisdictions and international forums.

    d. Dialogue with service providers and telecommunication companies.

    e. Related work and government priorities.

    f. Regulatory changes for law enforcement and/or the intelligence community to access data at or near the scale, timeliness, and reliability to address impact on investigations.

    g. Impact of any recommendations on:

        - ✓ The privacy, civil liberties, and human rights of targeted individuals and others;
        - ✓ Ensuring any approach considers all interests of or possible impacts on tangata whenua and the principles of Te Tiriti o Waitangi;
        - ✓ Commerce, economic competitiveness, and innovation;
        - ✓ International relationships; and
        - ✓ Overall security of New Zealand (e.g. preventing interventions that weaken cyber security overall)

**Peer Review**

10. The EWG, in consultation with the CSSCC, will invite independent Crown Entities, academics, the private sector, non-government organisations, civil society and community groups to review the draft report to ensure it includes all relevant benefits and costs of encryption.

11. The EWG will review recommendations from the peer review before submitting the final report to the CSSCC.