Privacy Commissioner's Submission to the Foreign Affairs, Defence and Trade Committee on the Asia-Pacific Economic Cooperation (APEC 2021) Bill (187-1)

Executive Summary

1. The functions of the Privacy Commissioner include examining new legislation for its possible impact on individual privacy. Central to that examination is the principle that policy and legislation should be consistent with privacy rights unless there is very good reason (and evidence) to override those rights.

2. The Asia-Pacific Economic Cooperation (APEC 2021) Bill ('the Bill') has been introduced to ensure that legal powers are in place to provide overall security for the Asia-Pacific Economic Cooperation forum (APEC 2021) events, to be hosted by New Zealand from December 2020. The legislation will be temporary for the purposes of APEC 2021 only and all provisions of the Bill will expire on 21 November 2021. Amendments made to other Acts will also self-repeal on that date.

3. My comments relate to Subpart 3 of Part 3 of the Bill, which enables the Commissioner of Police to authorise the New Zealand Police and foreign security agencies to import, use, and export wireless electronic countermeasure (W-ECM) technology during APEC 2021 events. W-ECM technology can detect, intercept, transmit, retransmit, disable, disrupt or interfere with radiocommunications. I understand that the Bill's provisions could allow for W-ECM technologies to intercept all radiocommunications (such as mobile phone and Wi-Fi networks) in an area and decrypt them if necessary.

4. I recognise the security implications of the APEC 2021 event and accept the need for limited W-ECM capabilities that have a low privacy impact, such as jamming radio communications the threat of remotely controlled bombs or drones.

5. However, I have three significant concerns about the W-ECM proposals:
   - i The Commissioner of Police will authorise W-ECM technologies without any ex ante independent judicial oversight and authorisation.
   - ii The proposals are disproportionate as they allow for the widespread interception of personal information of New Zealanders who are not suspected of being a security threat or of committing any offence.
   - iii Foreign security agencies using W-ECM technologies may not be subject to the same level of privacy protections as New Zealand law enforcement, and individuals are unlikely to be able to seek redress from them should their privacy be unjustifiably infringed.

6. To address these concerns about the privacy impact of the W-ECM proposals, I **recommend** the following changes to Subpart 3 of Part 3 of the Bill:
   - clause 92 is amended so that the use of W-ECM technology is subject to judicial oversight and authorisation, and

- clause 96 is amended to explicitly require W-ECM users to immediately cease their interception of personal information and to immediately destroy the personal information they have collected where they discover it is not useful to counter a potential or actual risk to security.

7. I also recommend a clarification to the drafting of clause 97 so that, for the avoidance of doubt, personal information collected through a W-ECM cannot be disclosed under an exception to the Privacy Act 1993.

The authorised uses and conditions of use of W-ECM in the Bill

8. Subpart 3 of Part 3 of the Bill provides that that the Commissioner of Police may authorise the use of W-ECMs by New Zealand Police and foreign security agencies during APEC 2021 in order to counter potential and actual risks to security. W-ECM is defined as any equipment or device that does any or all of the following: detect, intercept, disable, disrupt, or interfere with radiocommunications.

9. W-ECM authorisations can be for a planned use in a planned response (clause 93), or a reactive use where W-ECM are available to be used to react and respond to a certain type of radiocommunications as necessary (clause 94).

10. Clause 97 establishes the power to use authorised W-ECM and provides examples of the sorts of uses that W-ECM authorisations can be used for. Some of these applications may have limited or no privacy impact, such as:
    - locating the transmitter (remote control) of a drone by detecting and tracking the radio communications between the transmitter and a drone, and
    - jamming or distorting radiocommunications between a remote control and a bomb so the bomb does not detonate.

11. However, some W-ECM uses may have significant privacy impacts. For example, deceiving a drone so that radio-communicated instructions from a remote control are ineffective or overridden may require collecting a large amount of radiocommunications in order to identify the drone's radiocommunications.

12. Clause 96 sets general conditions on the use of W-ECM authorisations, including the secure storage, disposal of information and notification of affected persons to providers of existing services (for planned uses of W-ECM) and reporting any reactive use of W-ECM to the Commissioner of Police and the Radiocommunications Secretary. The Commissioner of Police may also impose other conditions that he or she thinks fit.

13. The framework and definitions used in subpart 3 are wide enough to encompass a number of surveillance and interception devices that could capture confidential private communications.

The judiciary should authorise W-ECM technology in the Bill

14. The absence of independent ex ante oversight and authorisation of W-ECM technology in this Bill is a deficiency that should be addressed. The power to use invasive W-ECM technology to intercept private communications should be subject to express restrictions and judicial scrutiny.

15. The judiciary has the necessary independence to assess broader considerations such as the principles of proportionality and minimising intrusion, while also having experience in interception and intelligence gathering matters.

16. The proposition that only the judiciary should authorise W-ECM technology is supported by analysis into 'data surveillance technology' by the Law Commission and Ministry of Justice in their review of the Search and Surveillance Act 2012[1]. Their report concludes that the ability to issue surveillance warrants should remain limited to judges.[2]

17. Most submitters to the Law Commission review felt that surveillance requires a higher level of oversight because it is a matter of public concern and can involve a substantial intrusion on privacy. Concern was also expressed that issuing officers who are not judges do not have the necessary legal expertise to give proper scrutiny to surveillance device warrants.[3] I note as well that the Commissioner of Police will be authorising New Zealand Police's use of W-ECM, a situation where there is no independent oversight at all.

18. Only two submitters, both enforcement agencies, favoured allowing officials other than judges to issue surveillance warrants. The submitters suggesting warrants could be issued more quickly, however neither suggested any timeliness issues had occurred when obtaining a warrant from a judge.[4]

19. If the Commissioner of Police was granted the power to authorise W-ECM, those decisions would be subject to oversight by the Independent Police Complaints Authority (IPCA). However, IPCA oversight is after the fact – it will be too late to undo potentially significant privacy intrusions arising from decisions that may be weighted towards operational considerations. The IPCA will also be ineffective with respect to devices deployed by foreign security agencies.

20. To address these concerns, I **recommend** that clause 92 is amended so that the use of W-ECM technology is subject to a warrant overseen by a judicial officer.

---

[1] Law Commission and Ministry of Justice, Report 141: *Review of the Search and Surveillance Act 2012* https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC-R141-Review-of-the-Search-and-Surveillance-Act-2012-final_0.pdf
[2] *Ibid.*, p.145
[3] *Ibid.*, p.145
[4] *Ibid.*, p.145

W-ECM technology in the Bill can harvest personal information indiscriminately

The proposed uses of W-ECM are disproportionate

21. I appreciate the justification for limited W-ECM capabilities that have a low privacy impact, such as jamming or distorting radiocommunications to mitigate the threat of remotely controlled bombs or drones.

22. My understanding is that to identify some threats, W-ECM technology will need to check all radio spectrum communications in specified locations such as security areas, secure transport routes, areas where protected persons will be – and adjacent areas to these areas. Checking for threats will require the interception and, if necessary, the decryption of personal information. This personal information may include emails and text messages and analysing the contents of those communications.

23. The W-ECM proposals will allow for the indiscriminate collection of communications of New Zealanders who pose no threat to an APEC event and are not suspected of committing any offence. The open-ended nature of the W-ECM authorising power and uses is disproportionate to the demonstrated need, given the W-ECM capabilities available that have a lower privacy impact.

Foreign security agencies using W-ECM raise additional privacy concerns

24. The Bill provides for the Commissioner of Police to permit foreign security agencies to intercept the radiocommunications of New Zealanders.

25. Foreign agencies represent a higher level of privacy risk as they may not be subject to the same level of privacy protections as their New Zealand counterparts. If personal information is collected by a foreign security agency and taken to their home jurisdiction, it will be entirely outside of the control of New Zealand agencies.

26. It is also unlikely that individuals will be able to seek redress from foreign security agencies should their privacy be unjustifiably infringed. While this would be difficult for the Bill to effectively address, the general conditions that W-ECM users are subject to should impose immediate constraints on their activities.

27. It is important that privacy protections in the Bill are clear and explicit so that foreign security agencies are subject to the same level of privacy safeguards as New Zealand law enforcement agencies.

The privacy concerns raised by W-ECM in this Bill can be further mitigated

28. The singular nature of the international event is insufficient to justify such unsupervised and sweeping powers to intercept and decrypt radiocommunications. The proposals should be redrafted to be more limited and contain greater safeguards.

29. There should be a clear requirement that W-ECM users immediately cease the collection of personal information if they discover it is not useful to counter a potential or actual risk to security. This requirement will reduce the amount of personal information unnecessarily collected by W-ECM users.

30. W-ECM's users should also be required to immediately destroy any personal information they have collected if it is not useful to a counter a potential or actual risk to security. This is tighter than the existing general condition in clause 96 to "dispose of the information as soon as it is no longer required for the purposes of that Act". Making this requirement stronger and more explicit will be especially beneficial with respect of foreign security agencies.

31. I **recommend** that clause 96 is amended to explicitly require a W-ECM user to immediately cease their interception of personal information and to immediately destroy the personal information they have collected where they discover it is not useful to counter a potential or actual risk to security.

Clarifying when personal information collected by W-ECM can be disclosed

32. Clause 97 constrains the disclosure of private communications[5] and personal information[6] to the following situations:
    - when it is authorised by another Act
    - when it is required to exercise a power or for a prosecution under the Bill
    - to another authorised W-ECM user for use in accordance with its use under clause 97, or
    - to the Commissioner of Police or the Radiocommunications Secretary for the purposes of reporting any reactive use of W-ECM.

33. I do not believe the intention of this clause is to allow for disclosures of personal information under information privacy principle 11 of the Privacy Act. However, as the drafting on this point is unclear, I **recommend** that clause 97 is clarified to explicitly note that disclosures of personal information under the Privacy Act are not allowed. This clarification will ensure that the extraordinary W-ECM powers are only used in situations considered by the Bill or as explicitly authorised by Parliament.

Conclusion

34. I trust my comments are of use to the Committee in its consideration of the Bill. I seek to be heard on my submission.

John Edwards
Privacy Commissioner
12 February 2020

---

[5] As defined in section 216A of the Crimes Act 1961
[6] As defined in section 2(1) of the Privacy Act