Privacy Commissioner
Te Mana Mātāpono Matatapu

Privacy Commissioner's submission to the Social Services Committee on the Deepfake Digital Harm and Exploitation Bill [213-1]

Introduction

1. I am pleased to provide a submission to the Social Services Committee (the Committee) on the Deepfake Digital Harm and Exploitation Bill (the Bill).
2. The Privacy Act 2020 is New Zealand's main privacy statute. One of the Privacy Commissioner's functions under the Privacy Act is to examine proposed legislation that may affect the privacy of individuals.
3. The Bill would amend section 216G of the Crimes Act 1961 (the Crimes Act) and section 4 of the Harmful Digital Communications Act 2015 (the HDCA) to expand the definition of an "intimate visual recording" to explicitly include images created, synthesised, or altered to show a person's likeness produced without consent.
4. For reasons set out below, I support the passage of this Bill as a step to better address privacy harms from deepfakes.
5. While out of scope for this Bill, in my view further policy work is needed to understand and address broader issues arising from synthetic media and related uses of generative AI tools. Failing to address these broader issues may contribute to significant privacy harms in New Zealand.
6. I trust my comments are of use to the Committee.
7. I do not seek to be heard on my submission but am happy to appear before the Committee if that would be of assistance.

Deepfakes raise issues for the privacy of individuals

8. Deepfakes are digitally generated or modified depictions of people in images, audio, or video.[1] Deepfakes can cause significant harms to individual privacy, including acute harms driven by sexualised deepfakes of women and children.[2]

9. The making and sharing of deepfakes can cause privacy harm in several ways:

    - **Collecting underlying personal information**: making deepfakes requires the use of existing images, video, or audio (real or otherwise) of the person depicted. To gather this personal information, people or agencies making deepfakes or deepfake tools may stalk or scrape social media and other sources. The personal information of people other than the subject of the deepfake may also be collected, for example, if their body parts are depicted or used in composite images or training data. Making deepfakes may also involve creating personal information.
    - **Processing personal information**: uploading personal information to chatbots or other tools may lead to onward sharing or reuse of information in training datasets or by other users.
    - **Sharing deepfakes**: having deepfakes circulated takes away a person's control of their personal information and knowledge of where it is held. It also takes away their control over how they are seen, attacks their dignity, and may undermine their relationships and standing in society.[3]
    - **Psychological harm**: a person seeing and hearing deepfakes of themselves may suffer direct psychological harm.

---

[1] Maher, Sean William, "Deepfakes", *Encyclopedia* 6 (4): 80, (2 April 2026), http://dx.doi.org/doi:10.3390/encyclopedia6040080

[2] See for example K Evans, "Deepfakes and privacy: it's time to respond" (January 2026), privacyfoundation.nz

[3] See Goodyear, Michael, Dignity and Deepfakes (March 31, 2025), 57 Arizona State Law Journal 931 (2025), http://dx.doi.org/10.2139/ssrn.5199514

- **Financial and reputational harms** can result from deepfakes being used to impersonate individuals or target them for scams or criminal activity including fraud and coercion.

10. The potential for these harms may also deter specific individuals, or groups of people, from participating in democratic processes and other aspects of life.

The Bill addresses some privacy harms from deepfakes

11. Existing Crimes Act and HDCA provisions criminalise the intentional or reckless making of an intimate visual recording of another person (s 216H of the Crimes Act), and the posting of an intimate visual recording without consent (s 22A of the HDCA).

12. The HDCA provisions were added by the Harmful Digital Communications (Unauthorised Posting of Intimate Visual Recording) Amendment Act 2022. The previous Privacy Commissioner provided a submission while those provisions were being considered at Select Committee in 2021. Some points from that submission remain relevant to addressing harms from deepfakes (which were not explicitly included in the 2022 amendment). In particular, the earlier submission made the point that in most cases the most immediate remedy the affected individuals will want is to have relevant content taken down and removed from circulation, a point I discuss further below.

13. The present Bill would extend existing offence provisions to deepfakes, specifically to "a visual recording that has been created, synthesised, or altered without the knowledge or consent of the person who is the subject of the recording".

14. The existing Crimes Act and HDCA provisions cover intimate images or recordings of intimate areas of a person's body.[4] As drafted, the Bill would not extend offence provisions to cover synthetic or altered images or recordings of the same intimate areas of a person's body. The Committee may wish to consider whether that aspect of existing offences should also be extended to cover synthetic or altered images or recordings.

15. I support the Bill. In my view this is a small but useful step to begin to address actions by individuals which can drive very significant privacy harms.

HDCA notice-and-takedown processes may benefit privacy

16. As the Privacy Commissioner's 2021 submission said, in most cases a main priority for affected individuals will be to have content taken down and removed from circulation. Enforcement of criminal offences and court orders under the Crimes Act and HDCA may be one way to address particular and serious cases of harm, but this requires formal legal processes and may not be the most appealing way for vulnerable individuals to respond when they are the subject of a deepfake.

17. As well as more formal remedies requiring a court process, section 24 of the HDCA provides a notice and takedown process, under which content hosts can avoid direct liability for a post by following specific process requirements. To benefit, a content host must pass on a complaint notice to the person who posted the communication complained about and must remove a post within 48 hours of receiving a complaint notice if the author (the content poster) does not respond. However, if the author does respond to a complaint notice passed on in this way,

[4] See Crimes Act s 216G(b) and HDCA s 4, definition of "intimate visual recording" at (a)(ii).

the content host would not be required to take down the content to benefit from section 24.

18. In principle, changes clearly bringing deepfakes in scope for this HDCA process may encourage content hosts to remove some deepfake content to avoid liability. This may help to reduce privacy harms to individuals.

19. While out of scope for this Bill, we suggest that further policy consideration should be given to the broader regulatory environment, including HDCA notice and take-down processes and accountabilities, to ensure that they are fit for purpose given the advent of synthetic media and AI generated content.

There is some potential overlap with the Privacy Act

20. Deepfakes are likely to involve personal information in terms of the Privacy Act.[5] The Bill's language of "the person who is the subject of the recording" means that the provisions addressing deepfakes are likely to relate to an identifiable individual. However, in my view the Privacy Act both requires amendment and cannot alone adequately address harms from deepfakes. This is because:

    - Responsibilities under the Privacy Act generally do not apply to individuals.[6] My understanding is that individuals are the main users of relevant tools and the main source of intimate deepfakes which would be in scope for this Bill.

[5] The Privacy Act applies to personal information, defined as information about an identifiable individual. Information privacy principle 7 provides a right for a person to correct personal information about them held by an agency, which implies that personal information includes false or inaccurate information about an individual

[6] Under section 27 of the Privacy Act, the information privacy principles have a restricted application to a person collecting or holding personal information solely for the purposes of or in connection with the person's personal or domestic affairs, unless the collection, use or disclosure would be highly offensive to a reasonable person. It is likely that the highly offensive threshold could be met by intimate deepfakes in at least some situations. However, processes and remedies under the Privacy Act may not be the best response available to affected individuals.

- The Privacy Act provides a constrained set of remedies which may not be a good fit for the deliberate and serious breaches of privacy arising from deepfakes. The 2021 submission mentioned in particular that there is no provision for a right to erasure or for civil pecuniary penalties under the Privacy Act. These are provisions that successive Privacy Commissioner's have advocated for.
- Processes for handling complaints under the Privacy Act include conciliation between parties as a preferred approach. This is likely to be inappropriate and potentially harmful in situations where privacy issues arise from deepfakes of an individual, particularly intimate deepfakes in scope here.

21. Individuals affected by deepfakes may choose to contact NetSafe as the approved agency under the HDCA, or to make a complaint to Police which could result in a prosecution. They may also make a privacy complaint to my Office.

Further policy work is needed to address broader issues

22. The Bill provides a small and useful improvement to legislation to better address harms from deepfakes where a criminal or court process can be effective.

23. This is only one part of the broader range of privacy harms that result or could result from widespread access to digital tools that make it easy to depict or impersonate individuals. Further policy work is needed to understand and address those broader issues, to ensure that online services uphold their responsibilities, and to provide better remedies for individuals who are harmed.

Conclusion

24. I support the Bill and **recommend** that it be passed.

Liz MacPherson
Deputy Privacy Commissioner

19 June 2026