# Regulatory Analysis Summary – Addendum

## Protecting sensitive information held and shared by the Regulator

### *Agency disclosure statement*

This regulatory analysis summary is an addendum to the Regulatory Impact Statement (RIS) *Reducing the risk of online harm to children: Phase One Policy Decisions* completed in March 2026.

This addendum was completed and reviewed by an independent panel in June 2026. The panel considers that the information and analysis summarised in the addendum partially meets the quality assurance criteria.

This addendum should be read in conjunction with that RIS. It compares the likely outcomes, costs, benefits, and risks of options to protect sensitive information that is held and may be shared by the Regulator in the course of its business.

This addendum examines three options (including the counterfactual) against criteria based on efficacy, building trust between the Regulator and age-restricted platforms, regulatory cohesion, and proportionality.

Limited timeframes have place constraints on our analysis. These constraints include:

- a lack of sufficient time to fully analyse the options to address the identified problem or provide a fulsome analysis of the benefits and costs
- officials have been unable to consult on the proposed options outside of standard agency consultation processes.

9(2)(a)

Proactively Released





Out of Scope

## *Background*

1. In March 2026, Cabinet agreed to progress Phase One of its two-step plan to improve children's online safety (by placing a minimum age requirement of 16 for accounts on social media and other platforms and child safety risk assessments on all under 18s) by developing a Bill [CAB-26-MIN-0098 refers].
2. A Regulatory Impact Statement (*Reducing the Risk of Online Harm to Children – Phase One Policy Decisions*) was completed for the initial policy decisions agreed to by Cabinet. That RIS provided more context and background regarding children's online safety and assessed options for both primary intervention and legislative design.
3. The draft Bill *Online Safety (Minimum Age and Child Safety Risk Assessment) Bill* (the Bill) seeks to implement Phase One and is required to be submitted to Cabinet for further consideration, prior to progressing any further [recommendation 6 of CAB-26-MIN-0098 refers].
4. In addition to seeking Cabinet's approval to introduce the Bill into the House of Representatives, the Minister will also be seeking Cabinet's agreement to several minor and technical policy decisions to improve the overall efficacy of the legislation. The majority of the additional policy decisions were exempted from regulatory impact assessment requirements. However, the Ministry for Regulation has advised that the proposal seeking to protect sensitive information held and shared by the Regulator requires further regulatory impact analysis.
5. Under the Bill, the Secretary for Internal Affairs is established as the Phase One Regulator, supported by the Department of Internal Affairs' Digital Safety Group.

## *Previous RIS Context*

6. New Zealand's current regulatory framework does not adequately safeguard children (under 18s) online, and it overlooks the heightened developmental vulnerability of children aged under 16. While some protections exist, there is no overarching framework that regulates social media platforms or other platforms where 'social' interaction (either with other users or Artificial Intelligence) occurs to prevent risk of exposure to harm.
7. If no action is taken, children's exposure to harmful content, contact and design driven-risks is expected to continue. Research shows that 24 percent of children aged 5–14 use social media, with usage rising sharply from age 9.[1] The Classification Office reports widespread concern about children's access to illegal or inappropriate content across social media and other online platforms.[2] New Zealand Police also report an average of ten sextortion cases each week, with 18 percent of victims under 17.[3] Together, these indicators show that without intervention, children will remain exposed to online environments where harmful content and contact can occur.

[1] New Zealand On Air, Where Are The Audiences - Children's Media Use Report, 2025.

[2] Classification Office, What We're Watching: New Zealanders views about what we see on screen and online, 2022.

[3] Police Association, NZPA: Sextortion: It's not just blackmail, 2024.





Proactively Released

Out of Scope

8. Emerging harms associated with AI-driven features are also expected to continue without regulatory intervention. Social AI companion chatbots are increasingly embedded in major platforms and can create dependency and inappropriate reinforcement. Without intervention, under-16s will continue to be exposed to these harms and reliance on voluntary platform action will remain. The risk of children moving into unregulated environments would also continue.
9. The benefits of removing under-16s' access to platforms outweigh the benefits experienced alongside continued exposure to online harm. Despite being one space for young people to connect, engage with others and information, it also exposes them to many harms including grooming, self-harm and suicide content, and algorithmic manipulation. This exposure to a range of harms is too great to continue to allow under-16s to have accounts on these platforms.

### *Counterfactual and problem definition*

10. Under the Bill's framework, the Regulator will be provided tools to gather and share information from any person (including both natural persons and legal persons) for the purpose of performing or exercising its functions and duties. These are standard regulatory tools and mirror those in the Commerce Act 1986.[4]
11. The Bill proposes that the functions of the Regulator are to:
    a. monitor and enforce compliance with this Act (including any secondary legislation made under it)
    b. promote education about, and awareness of, this Act and platform operators' duties under this Act
    c. publish guidance relating to this Act and information about the Regulator's regulatory activities, including monitoring, enforcement, and other compliance-related activities
    d. co-operate, and share information, with any law enforcement or regulatory agency or overseas regulator
    e. advise the Minister in relation to the making of regulations
    f. any other function conferred or imposed on the Regulator by legislation.
12. Under the Bill, the Regulator has the ability to compel any person to provide information if it is necessary or desirable to perform or exercise their functions, duties, or powers. The majority of persons who would be required to provide information to the Regulator would be operators of age-restricted platforms and their employees.
13. In the course of investigating compliance with the legislation, the Regulator will obtain information from platform operators that will likely contain sensitive information[5] regarding their age assurance processes, the design of their platforms and information on risks of harm present on their platform including their mitigation strategies.

[4] Section 98 of the Commerce Act 1986.

[5] Sensitive information in this context refers to information that is commercially sensitive, trade secrets, information about a platform's algorithms and information regarding how a platform detects and responds to harm on their services.



Out of Scope

Proactively Released

14. The Regulator may also share information it holds with other regulatory entities (such as the Classification Office), law enforcement (such as New Zealand Police) and overseas regulators (such as eSafety in Australia or Ofcom in the United Kingdom) if it is connected to their statutory role and responsibilities.
15. If this information were disclosed without protecting it, significant harm could occur. For example, during earlier targeted consultation on the primary proposals, platform operators informed us of their concern that practices and tools they use to detect and reduce illegal activity would be publicised and used by bad actors to get around them. This includes: significant financial harm to the platforms by leaking a trade secret to competitors or undermining potential business dealings; significant emotional and mental harm to individuals by disclosing information about potential criminal offending they were affected by; and undermine the Regulator's efforts to help reduce the risk of online harm on platforms by revealing potential investigations it has been pursuing.
16. Because of this high level of risk resulting from disclosure, platform operators will likely have significant concerns about providing the Regulator with sensitive information. Disclosure could also risk damaging the Regulator's reputation with the New Zealand public. A Regulator that is unable to keep sensitive information protected is unlikely to have the public's confidence that it can fulfil its responsibilities and may affect its ability to effectively co-operate with, and deliver education to, members of the public.
17. In these scenarios, the platform operator's trust that information will be appropriately protected is crucial to ensure the Regulator can effectively fulfil its role and responsibilities. Without a high level of trust, there is a risk that operators will be less forthcoming with providing information or may not provide the information at all. This information is critical for the Regulator to successfully complete investigations and undertake analysis of the online risk landscape, which are core parts of its responsibilities.

### *Objectives*

18. The objectives of this proposal are to ensure that sensitive information held by the Regulator is appropriately protected and create a high level of trust between the Regulator and operators of age-restricted platforms.

### *Options analysis*

19. The following criteria are applied to evaluate the relative strengths and limitation of each option against the status quo:

| | |
|---|---|
| • **Effectiveness** | The option protects information against intentional disclosure not associated with the Regulator's role and functions. |
| • **Enhancing trust** | The option builds and maintains trust between the Regulator and age-restricted platforms to continue the efficient flow of information. The option also builds trust between the Regulator and the public that the Regulator can effectively perform its functions. |





Out of Scope

Proactively Released

- **Regulatory cohesion** The option aligns with existing processes and legislative precedents.

- **Proportionality** The option is a proportional response to the risk of information being disclosed without authorisation and the harm that could result.

20. These criteria differ from the criteria in the March 2026 RIS due to the additional policy decision having different requirements to assess compared to the primary intervention options and broader design options assessed by the March 2026 RIS.
21. Effectiveness and enhancing trust will be given additional weighting as these criteria are the most important for achieving the objectives of the proposal.
22. An option to create a new civil duty of confidentiality is not being considered due to time constraints not enabling sufficient time to consider its implementation or interaction with the other clauses in the Bill.

***Option 1 – Counterfactual***

23. Under the counterfactual, there are some existing protections for information. For example, section 105A of the Crimes Act 1961 criminalises the use or disclosure of official information for an advantage or pecuniary gain. The Privacy Act 2020 provides protection of personal information[6] that is held and shared by entities, but it does not cover commercially sensitive information.
24. The Regulator could also rely on individual employment contract obligations to protect information or any information-sharing agreements or memorandums of understanding they may have with other law enforcement, regulatory entities, or overseas regulators.

**Option 2 – Criminally penalise information breaches (*preferred*)**

25. This option would place additional requirements in the legislation to protect against unauthorised disclosure or a failure to adhere to confidentiality requirements with criminal penalties if the requirements were not followed.
26. In practice, in the case of an unauthorised disclosure, the criminal mischief could include a person working for the Regulator intentionally leaking sensitive information to the public, or in the case of a failure to adhere to confidentiality requirements, an agency failing to properly secure sensitive information leading to unauthorised access.
27. These criminal offences would differ from the Crimes Act as it would not require a prosecutor to prove that an alleged offender used or disclosed information to obtain an advantage or pecuniary gain for themselves. In the context of the Bill, there are several circumstances where a person may disclose information without any intent of obtaining an advantage or pecuniary gain, which means the Crimes Act would not be contravened. This could include a person wanting to damage the reputation of a platform or accidental access or disclosure resulting from poor storage and security practices.

---

[6] Section 7 of the Privacy Act defines 'personal information' as information about an identifiable individual and includes information relating to a death that is maintained by the Registrar-General under Births, Deaths, Marriages and Relationships Registration Act 2021.



Proactively Released

Out of Scope

28. Additional protections for information in legislation are not unique and have been used in other contexts where the mishandling of information can cause significant harm to regulated parties. For example, the Financial Markets Authority Act 2011 places a prohibition against people working for the Financial Markets Authority (FMA) from publishing or disclosing information obtained whilst working for the FMA except in specified circumstances.[7] The Bill would authorise disclosure in the same circumstances.
29. Other legislation, such as the Overseas Investment Act 2005 and the Fire and Emergency New Zealand Act 2017, enables its regulatory bodies to place additional confidentiality requirements on information it holds or shares. These requirements can include maintaining the confidentiality of the information (particularly information that is personal information under the Privacy Act), ensuring the storage, use or access to the information is protected and requiring copying, returning or disposal of copies of documents provided.
30. Current criminal penalties for information breaches in legislation range from imprisonment to substantive fines. Under the Bill, criminal penalties would be limited to fines. Imprisonment would be disproportionate compared to the level of risk that information could be leaked and the level of harm that could result from the information being made public without appropriate protections.
31. The quantum of fine for an individual would be up to $100,000, or in the case of another entity, up to $4 million. This quantum has been chosen as it aligns with the tier three civil pecuniary penalties which are the lowest financial penalties under the Bill. Tier three penalties are designed to penalise non-compliance with the Regulator's power to require a platform to publish a formal warning or comply with a corrective notice. Comparatively, the quantum for similar offending under the Financial Markets Authority Act and the Overseas Investment Act is up to $200,000. The penalty for corrupt use of official information under the Crimes Act is up to seven years' imprisonment.
32. A person acting in good faith while exercising their legislative responsibilities, or if they had a reasonable excuse, would not be subject to a criminal offence. For example, if unauthorised disclosure was accidental and the person had relied on information or instructions from a trusted person in an authority position. These are common defences in legislation.
33. The specified circumstances for disclosure under the legislation also provides a defence for a person to rely on if they are required to disclose information under the Official Information Act 1982 or the Privacy Act.

**Option 3 – Waive civil liability protections for information breaches**

34. This option would have the protection against civil liability that is provided for all public service employees under section 104 of the Public Service Act 2020 removed in cases of failures to protect information held by the Regulator.
35. There is no legislative precedent for civil immunity under the Public Service Act being removed.

[7] Circumstances include disclosing or publishing information to the FMA itself, as directed by the FMA or in accordance with the Official Information Act 1982 or the Privacy Act.



Out of Scope

Proactively Released

36. Waiving civil liability protections would expose the Regulator and its employees to potential civil litigation by operators of age-restricted platforms when an information breach occurs. This would enable operators to seek potential damages or restitution directly from the Regulator for any harm resulting from the mishandling of information they have provided to the Regulator.
37. Similar defences available under Option 2 would be provided for people acting in good faith or if they have a reasonable excuse.

Proactively Released



Out of Scope

| | Option 1 – Counterfactual (Rely on Crimes Act and standard contractual protections) | Option 2 – Criminally penalise information breaches more broadly (*preferred*) | Option 3 – Waive civil liability protections for information breaches |
|---|---|---|---|
| **Effectiveness** | **0**<br>Crimes Act offences protect against corrupt use and disclosure of official information, but it is limited. Standard employment contracts and information-sharing agreements have clauses that place protections on information held and/or shared to incentivise correct handling. | **+**<br>Criminal penalties under the Bill would protect unauthorised disclosure in more circumstances compared to the counterfactual (consistent with the policy) and would protect against poor confidentiality requirements.<br>This option place strong incentives on the Regulator to ensure information is tightly protected. | **+**<br>Civil liabilities would place a similar incentive to criminal penalties but may be less due to the consequence of not having a criminal record as a result of mishandling. However, removing civil liabilities would cover a broader range of behaviours than just 'corrupt use or disclosure.' |
| **Enhancing trust** | **0**<br>Imprisonment is a significant punishment, but it is limited to circumstances where an advantage or pecuniary gain can be proven.<br>It is unlikely that potential employee dismissal or revocation of an information-sharing agreement would be enough to encourage trust from platform operators. | **+**<br>Broader criminal penalties are more likely to give platform operators the confidence that their information will be protected and that there will be significant consequences for misuse. More likely to strengthen public confidence in the Regulator's use of information gathering powers and ability to respond to misuse. | **0**<br>Civil liability may provide some confidence to platform operators, but it is unlikely to be equivalent to the confidence from criminal penalties. Civil litigation can be complex and time-consuming. |
| **Regulatory cohesion** | **0**<br>Additional legislative protections for the handling of sensitive information are not mandatory in all frameworks. The counterfactual relies on existing legislation to prevent the misuse of official information. | **+**<br>Other frameworks handling similarly sensitive information have adopted criminal penalties to protect information, but it is not ubiquitous. | **- -**<br>Waiving civil immunity is novel and untested. It could expose the Crown to significant financial liability and have a chilling effect on the Regulator's willingness to enforce the regime (if it is exposed to uncapped liability). |
| **Proportionality** | **0**<br>Imprisonment is proportionate for corrupt use of official information but is likely disproportionate in other circumstances.<br>Employee dismissal or revoking an information-sharing agreement will have some impact but it will be limited to the individual and Regulator's reputation. | **+**<br>Criminal penalties for mishandling information may be seen as a disproportionate response, but this can be mitigated through defences, not having imprisonment as a possible penalty and ensuring the quantum of any maximum fine is commensurate to the potential risk and harm involved. | **-**<br>Although the Regulator would not be subject to criminal penalties, platform operators could seek significant financial damages from the Regulator.<br>For example, the leaking of a trade secret from a major platform could cause significant financial losses which they may seek to recover from the Regulator. |
| **Overall analysis** | **0**<br>Criminalising corrupt use of official information incentivises trust in limited circumstances and protections against mishandling of information in contracts and information-sharing agreements are acceptable. However, given the types of information being obtained by the Regulator, standard protections are unlikely to be sufficient to create a high-trust environment. | **4**<br>Broader criminal penalties for protecting and incentivising the correct handling of information are common and more appropriate when the information is sensitive. Broader criminal penalties will create a high level of trust between the Regulator and platform operators compared to the other options. | **-2**<br>Waiving civil immunity is novel, is unlikely to provide the same level of trust compared to criminal penalties and exposes the Regulator to potentially uncapped financial liability that risks the efficacy of the Bill's framework. As it is novel, untested and may raise constitutional issues, it inherently brings uncertainty. |

Out of Scope **od** **0 Neutral** **- Poor** **- - Very poor**

Proactively Released

### *Conclusion*

38. Based on the analysis, option 2 is preferred. The Minister agrees with this approach and has agreed to the introduction of criminal penalties to ensure sensitive information held and shared by the Regulator is protected.

39. Adopting broader criminal penalties for the mishandling of information creates the strongest incentives to protect sensitive information compared to the counterfactual, and in turn, will cultivate the highest level of trust between the Regulator and operators of age-restricted platforms. A high level of trust and protection will ensure that the Regulator can effectively obtain information necessary to fulfil its role and responsibilities and efficiently investigate non-compliance with the legislation.

40. Option 2 would create the highest level of trust between the Regulator and the public. Broader criminal penalties would strengthen the public's confidence that the Regulator would responsibly use its information gathering powers and would take and respond to information breaches seriously.

41. Option 2 would also support the Crown's role as a Te Tiriti partner. Māori data is considered taonga which the Crown has a duty to protect (as per Waitangi Tribunal claim 262). Broad criminal penalties provide the strongest protections out of the options assessed, which was supported by Te Puni Kōkiri during agency consultation.

42. Criminal penalties can be made more proportional by ensuring that the fines are linked to similar offending in other legislative regimes and within the Bill itself. As well, providing defences for acting in good faith or where there is a reasonable excuse helps protect the Regulator, its employees, its agents, and entities it shares information with from liability in instances where proper processes have been followed. This also prevents the criminal penalties from having too much of a chilling effect on the Regulator performing its responsibilities.

### *Risks associated with the preferred option*

43. The preferred option does present some risks. Confidentiality requirements placed on information that has been shared with other entities has the potential to limit what the other entity can do with that information. Following consultation with the Classification Office, it expressed concerns that criminal penalties may impact its ability to use or disclose shared information for a different purpose if it is connected to its legislative functions. This risk can be mitigated by clarifying how additional use and disclosure of information would operate through a memorandum of understanding between the Regulator and another entity or by updating the specified circumstances in the Bill to include instances where use or disclosure is authorised by other legislation. However, the latter option does risk weakening the protection the criminal offences provide.



Proactively Released

44. Another risk is the legislation's limited application outside of New Zealand. The Regulator will likely be sharing information with overseas regulators (such as eSafety in Australia or Ofcom in the United Kingdom) as part of its functions. If unauthorised disclosure or a confidentiality breach were to occur, it is very unlikely that the employees of the overseas regulators could be prosecuted. This risk is mitigated by many overseas regulators' countries having their own legislation criminalising unauthorised disclosure. For example, Australia criminalises unauthorised disclosure through their Criminal Code and the United Kingdom criminalises the misuse of official information through their Communications Act and Official Secrets Act.
45. International co-operation and information sharing relies on comity between regulators to be effective. An information breach can significantly affect the relationship and the likelihood that further information will be shared. This risk creates an incentive to protect information that has been shared internationally.

### *Expected additional benefits and costs of the preferred option*

46. Due to limited timeframes, a full analysis of the preferred option's benefits and costs could not be completed. However, we have analysed what we consider to be the primary benefits and costs.

*Benefits*

47. Under Budget 26, the Government has committed $30.75 million over the next four years to reducing the risk of online harm to children, subject to future policy decisions. This funding is intended to establish the Regulator's capability and ongoing regulatory work. By ensuring that the Regulator can effectively perform its role, functions and responsibilities, the preferred option helps protect this significant Government investment in reducing children's online harm.
48. By creating strong incentives to protect information provided to the Regulator, operators of platforms have a significantly reduced risk that their commercially sensitive information becomes public. Platform trade secrets, such as their algorithms, are their most valuable assets and every year platforms invest heavily into their research and development. For example, in 2025, Alphabet (operator of YouTube) invested approximately $61.087 billion (USD)[8] and Meta (operator of Facebook and Instagram) invested approximately $57.372 billion (USD)[9] in research and development. The preferred option helps protect this significant investment for platforms.
49. An additional benefit of the preferred option is that it provides protection for the Regulator and others by clearly defining when disclosure is and is not allowed. This way, the Regulator, its employees, its agents, and entities it shares information with can operate with confidence that, if they are following the legislation, they will not be subject to any penalty. This provides beneficial regulatory certainty. An absence of defining unlawful disclosure could expose the Regulator to uncertainty and risk if challenged by a platform operator. This would have a chilling effect on the Regulator's exercise of its functions.

---

[8] Alphabet Annual Report 2025 at page 49.

[9] Meta Platforms Annual Report 2025 at page 89.



Proactively Released

*Costs*

50. An individual who contravenes the new criminal offences created by the preferred option could be subject to a $100,000 fine. This is the maximum amount for a fine, and an individual may have to pay significantly less depending on the circumstances of the offending. An individual may also lose their job and future potential job opportunities as a result of being convicted. However, an employee of the Regulator losing their job due to a major information breach is a likely cost regardless of whether there are criminal penalties.
51. If the Regulator or another entity under the Crown contravenes the new criminal offences, they could be liable to a $4 million fine. This is the maximum amount for a legal person (i.e. anyone other than a 'natural person') under the legislation, and an entity may have to pay significantly less depending on the circumstances of the offending.
52. Private entities, such as a firm hired to audit a platform's age assurance processes, could also be subject to a fine and the impact of having any contract with the Regulator cancelled. A private entity that has an information breach is likely to suffer significant reputational loss which could affect its ability to secure future Government contracts.

### *Monitoring, evaluation, and review*

53. Monitoring, evaluation, and review of the preferred option will occur through the Regulator's annual report processes. The Regulator will report on compliance with its legislative obligations, including any disclosure of information that it has obtained from operators whilst fulfilling its role and responsibilities.
54. The Bill also includes a requirement to review its operation and effectiveness within a set time of within two years. This review provides an opportunity to consider if criminal penalties for mishandling information are working as intended.

Proactively Released



Out of Scope