Submission: Safer Online Services and Media Platforms

Introduction

1. We welcome this opportunity to submit on the Safer Online Services and Media Platforms discussion document.

2. The discussion document proposes an updated model for content regulation, responding to digital technologies and a media environment characterised by interactivity, multidirectional flows of information, and mingling of professional with personal content. Aspects of this media environment are supported through the pervasive collection and use of personal information, including for tracking, analytics, and advertising. In this environment, challenges for content policy are deeply interwoven with the need to uphold human rights including privacy.

3. Data from media platforms is used to inform online advertising and content curation, for general research purposes, and in particular for training algorithmic and "AI" systems, which are a focus area for our privacy work. Biases in online interactions affect privacy interests in accuracy, transparency, and fairness both directly and as a data source.

4. A key proposal is the creation of a new regulator to oversee the content regulatory system, which would operate alongside existing bodies including our office.

The role of the Privacy Commissioner

5. Under the Privacy Act 2020, the functions of the Privacy Commissioner include examining new legislation for possible impacts on individual privacy. We also have a role monitoring emerging privacy issues, and offering guidance on how people in industry, government agencies, and across broader society can uphold privacy.

6. Our aim in this submission is to ensure that an updated content regulatory framework will help to uphold privacy interests and complement our work. Privacy regulation is an important part of the human rights system and the broader regulatory framework which upholds the interests of New Zealanders. Privacy protections are important in their own right, but also work to enable the exercise of other rights and to prevent other kinds of harm across the economy, for example by enabling access to information about us held by online services and media platforms. In the current environment, we are paying particular attention to privacy impacts of digital technologies.

7. We address the consultation questions at the end of this submission. Below we respond to the key privacy issues raised in terms of:

    - Ensuring proposals are compatible with the existing privacy framework
    - Building privacy protections into the proposed regulatory framework
    - Opportunities and best practices for the proposed regulatory framework

Ensuring proposals are compatible with the existing privacy framework

8. The proposed content regulation model will sit alongside the privacy framework and may overlap with it. In general, privacy protections and obligations under the Privacy Act apply to any person or organisation when collecting, using, or disclosing personal information. This broad scope is important to uphold privacy expectations and best practices across the economy. Potential overlaps include the following:

    - Some activities of online services and media platforms may be subject to both frameworks (and potentially to other regulatory frameworks as well);
    - Some specific situations may give rise to both privacy harms and content harms (eg if a security breach enables impersonation or targeted misinformation);
    - Members of the public will need to navigate both frameworks (eg when seeking information or raising specific issues for investigation).

9. Some of these overlaps will need to be considered in designing the broader structure of the proposed content regulatory framework, others at the operational stage. This framework and the Privacy Act will need to complement each other, and we are keen to help with that. At the operational stage, there may be opportunities to coordinate on communications and educational materials to help members of the public understand both frameworks.

10. We would welcome work to coordinate on the handling of complaints and compliance activities, so that everyone is clear which areas fall to which regulator and how to handle overlaps efficiently. The handling of referrals and transferred complaints may need particular attention in the privacy context, as our work is governed by secrecy requirements under s 206 of the Privacy Act.

11. The Privacy Act also provides a model to consider in designing aspects of the proposed content framework. The information privacy principles provide general privacy standards which can be modified to apply to specific industries and situations by Codes of Practice. These codes are designed by the regulator in consultation with relevant industry and community bodies, a process which can be initiated on request or by the regulator.

12. One way the Privacy Act deals with broader public interests is through specific exceptions to its requirements for certain areas (e.g. news media). We think the proposed content regulatory framework may interact with the news media exception and the domestic affairs exception in ways that need attention.

13. The news media exception recognises the special role of news media in a democratic society, excluding news activity from the Privacy Act where media regulation provides

effective oversight of the relevant news entity.[1] The current law refers to the oversight of the Broadcasting Standards Authority (the BSA), the New Zealand Media Council, an overseas regulator, or another body prescribed in regulations.[2] Proposed changes including removing the BSA will require updates to this definition. We recommend carefully considering the desired scope of a news media exception, and ensuring that this privacy exception will continue to (a) apply only to news activity and not to other activity by media organisations and (b) require adequate regulatory oversight.

14. The domestic affairs exception limits privacy obligations for individuals who collect and use information solely for a personal or domestic purpose. This exception recognises that applying privacy obligations in that context may be impractical and intrusive. The Harmful Digital Communications Act 2015 modified this exception so it does not apply where the collection, use, or sharing of personal information would be highly offensive to a reasonable person.[3] This change recognised that digital sharing can have a persistence, speed, and reach that enables serious harms to privacy, and may blur the bounds of personal and public sharing. It enabled the privacy framework to respond where, for example information was obtained in a domestic situation and then later shared online without consent. These situations will overlap with the content framework.

Building privacy protections into the proposed regulatory framework

15. The proposed regulator will need to collect, use, and disclose personal information on a large scale, and may need information gathering powers in respect of online services and media platforms that hold vast quantities of personal information on New Zealanders. Ensuring that the regulator establishes a privacy protective culture is therefore crucially important. We strongly recommend that detailed and independent privacy impact assessments (PIAs) are commissioned to inform the design of the regulatory system, and also the design of any industry codes to be developed. We also recommend planning for work to revise and update these PIAs over time. This is a chance to apply privacy best practice.

16. The proposed regulator will take on the roles of existing bodies including the Chief Censor's Office and the Broadcasting Standards Authority. It will be important to consider the privacy impacts of transferring information from those bodies, and how this information should be governed to maintain expectations of privacy.

17. The proposed framework covers online services and media platforms all of which rely on collecting, processing, and disclosing personal information to function. The content layer of posted content and connections relies on back-end handling of names, email addresses, passwords, device identifiers, trackers, and other personal information, all of which needs to be handled in compliance with the Privacy Act, including for overseas

---

[1] Roth PA7.16
[2] Privacy Act s 7, definition of "news entity".
[3] Privacy Act 2020 s 27(2), originally due to the Harmful Digital Communications Act 2015.

entities such as major online services. We recommend approaching new responsibilities under the proposed content framework and any industry codes in a way that will reinforce and complement robust privacy protections. Regulatory coordination is important, particularly for overseas entities.

18. Overseas, there are policy proposals related to online safety which include aspects that would have a serious, broad, and negative impact on privacy and other human rights. We would urge caution on measures that require widespread collection and sharing of more personal information, such as mandated ID checks, or which limit people's online privacy, for example by restricting access to private messaging. These measures inherently harm privacy, and also expose people to increased cybersecurity and data breach risks. Some overseas policy proposals are presented in the context of protecting children from harm online, an area we address in more detail below.

19. We also urge caution around proposals for technological remedies, such as mandates that an Internet service provider block access to a particular website or service. Policy interventions at the technology level are a blunt tool and break the normal end-to-end connectivity of the Internet protocol stack. Disrupting normal Internet connectivity can affect online privacy by breaking the normal security model of encrypted traffic, by centralising data in a way that enables surveillance and presents a target for hacking, and by encouraging people to adopt less-secure practices like using free VPN tools which may aggregate and on-sell web traffic information. We would prefer to see remedies that uphold transparency and due process, like enforceable takedown notices.

Privacy issues for children and young people

20. One consideration is how the proposed framework would apply to children (people under 18), who are increasingly involved in digital environments. Our May 2022 Insights Report shows that second only to concerns about 'businesses sharing personal information without my permission' were concerns relating to 'information collected about children online without parental consent'. The concern rated third was 'security of personal information on the internet', which also affects children.

21. The Privacy Act 2020 has general application to children. Children are also specifically mentioned in IPP4(b), s 49, and 116. While these provisions are 'protective' in nature, all avenues of privacy complaint or dispute resolution can be accessed by children. Our new powers and compliance functions under the Privacy Act 2020, particularly the mandatory breach reporting requirement, have given us additional insights into the operation of dispute resolution schemes in relation to children and young people.

22. We are putting a deliberate focus on children's privacy issues. We have established a priority project focused on children and young person's privacy issues, including privacy issues faced online. The aim of the project is to ascertain whether regulatory changes are needed to better support children's right to privacy.

23. Bearing these issues in mind, you may wish to consider at the outset how the proposed regulatory framework will to apply to children, particularly in relation to:

    - The general applicability of the rules to children as heavy users of online resources and platforms;

    - Whether children will have access to any dispute resolution mechanisms in their own right to make complaints and report breaches and have these investigated where appropriate;

    - How the proposed regulatory framework will ensure that children's privacy is protected in the administration of the framework noting that gaining trust and confidence of children and their whānu users and the wider public will be critical to the framework's effectiveness as a regulator, particularly in relation to any complaints or dispute resolution process.

24. As our Children and Young People's Privacy project develops over the next 12 months, we will keep in touch, to help to inform the alignment of the proposed framework with considerations around the privacy regulatory environment for children.

Opportunities and best practices for the proposed regulatory framework

25. Designing a new regulator is a chance to improve the regulatory system, and to align with existing regulators around public communications, insights on systemic issues, and coordination on operational matters such as handling complaints. We would welcome the new regulator taking an active leadership role in these areas rather than leaving them to ad hoc coordination across the spectrum of online and media organisations. Having one point of contact would be beneficial from a regulatory perspective as well as from a public communications perspective.

26. Our experience is that complaints are one important source of information, but following complaints alone is not the best way to get early and relevant information on systemic issues. We recommend you look at ways to include expert and community perspectives on emerging issues at the top level of the framework, perhaps through an advisory panel. As well as helping to inform systems-level regulatory thinking, this would also be an avenue for ensuring the framework is transparent, accountable, and relevant for New Zealanders.

Conclusion

27. Thank you for the opportunity to submit on this process. Privacy interests are important in their own right, and contribute to the safety and participation interests this framework aims to protect. We see a chance here to uphold existing privacy protections, to build privacy protections into the proposed framework, and to consider opportunities to develop privacy best practice across the regulatory system.

Ngā mihi nui,

Michael Webster
Privacy Commissioner

Consultation Questions

Definitions in the proposals

1. What do you think about the way we have defined unsafe and harmful content? (page 18)

The proposed definitions focus on the experience of content by a person, either actual (harmful content causes harm when experienced) or hypothetical (unsafe content would risk causing harm if experienced), in terms of an open-ended list of interests. Compared with the privacy framework (which has the definition of 'personal information' at its core), these definitions are subjective and open-ended, which may present challenges to understanding the scope and nature of rights and responsibilities under the framework.

The focus on harm from experiencing content may exclude situations where people desire to see content that at a systems level presents risks to broader interests such as social cohesion and trust in shared social institutions, such as public health measures or electoral processes, and it may be intended that this would be in scope. It might be helpful to develop a more concrete list of interests affected, perhaps by reference to the Information Privacy Principles, the Human Rights Act 1993, and the Communication Principles at s 6 of the Harmful Digital Communications Act 2015.

2. Does the way we have defined unsafe and harmful content accurately reflect your concerns and/or experiences relating to harmful content? (page 18)

Our focus is on upholding privacy interests. The key definition in our framework is personal information, which is information about an identifiable individual. This is a relatively clear and concrete definition, though what is "identifiable" may depend on context. It may be a challenge to develop a similar definition for the proposed content regulatory framework.

About our proposed new framework to regulate platforms

3. Have we got the right breakdown of roles and responsibilities between legislation, the regulator and industry? (page 32)

We support proposals for a new, independent regulator to oversee the whole content regulatory system. The Privacy Act sets general standards in legislation, and allows for development of industry codes to apply those standards to specific contexts. This may be a useful comparison for content regulation.

It is important that the development of industry codes is not solely driven by industry, but reflects community needs and the broader public interest. Our experience is that the ability to participate in policy development processes is very uneven across communities, and the communities with most at stake are often least able to participate. We would welcome consideration of how to support and resource community participation at all stages, as this is critical to the relevance and credibility of any standards adopted in industry codes.

4. Do you agree that government should set high-level safety objectives and minimum expectations that industry must meet through codes of practice? (page 32)

We agree that high-level safety objectives and minimum expectations should be set in legislation. It is important that these expectations are set in legislation rather than by government agencies, to offer clarity across the regulatory system, and to protect the independence of the new regulator which will oversee the framework.

5. Do you agree with how we have defined 'platforms'? Do you think our definition is too narrow, or too broad? If so, why? (page 32)

We do not have a definite view here.

6. We are trying to focus on platforms with the greatest reach and potential to cause harm. Have we got the criteria for 'Regulated Platforms' right? (page 32)

Setting a threshold based on size and reach seems like a reasonable approach, comparable to the domestic purposes exclusion in privacy law. We think particular care is needed around measures for content that is intended to be private, or limited to a particular audience, such as one-to-one and group direct messages, as distinct from public material.

7. Do you think we have covered all core requirements needed for codes of practice? (page 39)

To gain trust as a regulatory tool, codes of practice may need to be led by the regulator and communities rather than industry, though industry should inform technical requirements.

8. What types of codes and industry groupings do you think should be grouped together? (page 39)

Key distinctions include the size of services, how much they emphasise user-generated material, how they curate content, and aspects of their business models. We have a particular interest in platforms and services that gather and process large amounts of personal information, but these may not map neatly onto categories based on the type and presentation of content. Many media platforms and online services may interact with online advertising markets on the back-end, in ways that are not transparent to users.

Where there is a choice of how to group services, we would prefer groupings that have similar privacy impacts (eg large overseas-based social media services) or fall under specific areas with recognised public interest considerations (eg news media and journalism). However, it is worth being cautious about whether every activity undertaken by an entity is related to its nominal category – for example general marketing activity is not news activity.

9. Do you think some types of platforms should be looked at more closely, depending on the type of content they have? (page 39)

A risk-based approach makes sense, and this could depend on the behaviour of platforms and the content they orient around in ways that go beyond their size and reach, and which may change over time. In the privacy context, one specific concern would be platforms encouraging or condoning "doxxing" of particular people or communities (sharing a person's address or other details for the purpose of harassing them). A pattern of enabling or encouraging this behaviour might be a high risk and harmful activity even on a small platform, and might deserve compliance action on both privacy and content grounds.

10. Do you think the proposed code development process would be flexible enough to respond to different types of content and harm in the future? Is there something we're not thinking about? (page 43)

Our operational experience is that complaints alone do not give enough information to identify and address systemic risks as a regulator. We think that strategic information-gathering should be built

into the structure of the regulator. This could include establishing a community oversight body to inform the operation of the framework as a whole.

One of the key challenges will be ensuring effective compliance practices at the various levels of the framework, from media organisations up to the regulator. We would encourage an approach where the regulator takes a strong leadership and guidance role, and perhaps offers a point of contact for the public and for regulatory coordination. This might help with quicker responses to systemic and emerging issues across the content system.

11. What do you think about the different approaches we could take, including the supportive and prescriptive alternatives? (page 43)

We support the approach proposed for this evolving area of regulation. The supportive approach risks leaving serious and systemic harms in place without a remedy. The prescriptive approach would risk locking in specific regulatory requirements that over time will either over-regulate or become irrelevant as technology, business models, and cultural practices change. Each approach should be applied according to the appropriate context, with a focus on which best addresses the identified harm in a proportionate and effective manner.

12. Do you think that the proposed model of enforcing codes of practice would work? (page 48)

We support proposals for compliance notices, and for financial penalties where regulated platforms do not comply. Proposals for access and service restrictions present serious concerns from a rule-of-law and human rights perspective, and depending how they are implemented may directly or indirectly pose risks to privacy. Technical measures to restrict access to specific online services may require breaking the normal end-to-end security of Internet connections, and may drive people to use VPNs or other tools that present their own privacy risks. We would urge caution for New Zealand as a democratic nation that has committed to a free, open, and secure Internet adopting this kind of enforcement tool.

13. Do you think the regulator would have sufficient powers to effectively oversee the framework? Why/why not? (page 48)

We would hope to see the potential for significant and financial penalties at a level relevant to the scale of regulated organisations, and by comparison with overseas frameworks.

14. Do you agree that the regulator's enforcement powers should be limited to civil liability actions? (page 48)

We would recommend considering a range of regulatory tools to achieve the goals of the framework. Financial liability should be informed by looking at the scale of penalties imposed on digital services overseas for significant breaches of privacy and other interests.

15. How do you think the system should respond to persistent non-compliance? (page 48) 16.

We favour responses that uphold rule-of-law expectations around due process and transparency rather than technical-level interventions.

16. What are your views on transferring the current approach of determining illegal material into the new framework? (page 54)

Our interest here is to ensure that information transferred from existing regulators maintains privacy expectations as the new framework is put in place.

17. Should the regulator have powers to undertake criminal prosecutions? (page 54)

We do not have a definite view here.

18. Is the regulator the appropriate body to exercise takedown powers? (page 56)

Locating enforceable takedown powers with an independent regulator would be an improvement on DIA holding them. Their use by the regulator should be subject to further oversight. This may be a potential role for a community advisory panel.

19. Should takedown powers be extended to content that is illegal under other New Zealand laws? If so, how wide should this power be? (page 56)

This is an area that needs further discussion to test the appropriate scope with regulators, industry, civil society, and community groups.

20. If takedown powers are available for content that is illegal under other New Zealand laws, should an interim takedown be available in advance of a conviction, like an injunction? (page 56)

Interim takedowns may be awkward, given the potential difficulty of restoring content, and this may have impacts on accuracy and access to personal information.

Potential roles and responsibilities under the proposed framework

21. What do you think about the proposed roles that different players would have in the new framework? (page 63)

We think that it may be sensible for the regulator to host the development of codes, which in practice will be strongly influenced by and implemented by industry in any case.

22. Have we identified all key actors with responsibilities within the framework? Are there any additional entities that should be included? (page 63)

Our office and other relevant regulators are key players to consider, including with respect to overlaps in responsibilities, operational matters, and public communications.

What would the proposed model achieve?

23. What do you think about how we're proposing to provide for Te Tiriti o Waitangi through this mahi? Can you think of a more effective way of doing so? (page 69)

We welcome consideration of Te Tiriti in the the design of this framework. We agree Māori should be represented in the framework.

24. Do you think that our proposals will sufficiently address harms experienced by Māori? (page 69)

It will be important to work with Māori to understand these issues and design an appropriate framework. We have a developing programme of work to do this in the privacy area.

25. What do you think about how rights and press freedoms are upheld under the proposed framework? (page 70)

We think it is critical to consider privacy across the design of the framework, and to build requirements for privacy assessments into the process for developing industry codes. Privacy is a human right which sits alongside and supports free expression, safety, public participation, and accountability of institutions to the people they serve.

We see particular overlap with news media exception under the Privacy Act. This excludes from the Privacy Act news activity by a news entity subject to adequate media regulation. We recommend carrying over that exception, with attention to ensure that only news activity is covered, and that covered news activity is subject to adequate regulatory oversight to serve the public interests which news media contribute to.

26. Do you think that our proposals sufficiently ensure a flexible approach? Can you think of other ways to balance certainty, consistency and flexibility in the framework? (page 70)

We recommend consideration of ways to effectively include community perspectives on systemic and emerging issues across the framework. One way to do this would be to create a community advisory panel to inform the top-level operation of the framework.