Privacy Commissioner
Te Mana Mātāpono Matatapu

Privacy Commissioner's submission to the Education and Workforce Committee inquiry into the harm young New Zealanders encounter online, and the roles that Government, business, and society should play in addressing those harms

1. I am pleased to provide a submission to the Committee's inquiry into harms young New Zealanders encounter online.

2. The Privacy Act 2020 is New Zealand's main privacy statute. Among the Privacy Commissioner's functions under the Privacy Act are examining proposed policies and technological developments that may affect the privacy of individuals.

Executive summary

3. The online world provides both opportunities and risks for young people. While the benefits for young people of being online should not be ignored, the risks are significant. Young people must be protected online, and regulation plays a very important role in keeping them safe. However, regulation needs to be appropriately targeted, effective and proportionate in relation to the harms it seeks to address.

4. Among the risks young people encounter online are risks to their privacy. When young people go online, their personal information is likely to be collected, used and shared in ways they are not aware of, and that can have real impacts on them. Those impacts can include targeted marketing, online scams or predators, cybersecurity threats such as phishing or malware, and online bullying. The increasing use of artificial intelligence online is also creating new risks and worsening existing ones.

5. Young people's privacy is a significant concern for New Zealanders. In a 2025 survey conducted for my Office, 67% of New Zealanders were concerned about the privacy of children, including when they use social media. Because of public concern and the vulnerability of young people to online privacy risks, my Office started a project on children and young people's privacy. The project is currently focusing on producing guidance to help young people and their whānau, and people who work with young people, to understand how best to protect young people's privacy rights.

6. While guidance can help individuals to navigate the challenges of safeguarding young people's privacy, collective responses through regulation are also needed. One possible regulatory response that is currently the focus of considerable discussion is banning young people from accessing certain online platforms. In particular, there are current proposals to ban those under 16 years of age from having social media accounts.

7. I understand and support the desire to protect young people from online harms that lies behind proposals for age restrictions, and I recognise that these proposals appear to have significant public support. However, such restrictions would involve privacy and other risks. I am unable to support proposals to ban young people from online platforms until a robust policy case, including full consideration of implementation issues, has been prepared.

8. From a privacy perspective, the main concern with age-restricted access to online platforms is the means by which age will be verified online. Age restrictions require *all* users of online platforms to verify their ages, and age verification can involve the collection of sensitive identity information about individuals. Collecting identity information about every New Zealand user of online platforms would create significant risks of over-collection of personal information and the creation of 'honeypots' of identity data that could be stolen and used by fraudsters and identity thieves. Using facial analysis to detect age also raises concerns about collecting sensitive biometric information, as well as risks of inaccuracy.

9. At the same time, I acknowledge that age verification technologies are continually advancing, and that it may be possible to find a solution which simply verifies that a person is, or is not, aged 16 or over, without collecting other information about the person. The Digital Identity Services Trust Framework is a legislatively-mandated framework for safely sharing information in a digital form, and the option of integrating any future age-verification system into this framework should be seriously explored.

10. Before any legislation to ban young people from online platforms is progressed, the following steps are necessary:

    - A thorough policy analysis should be carried out, including assessment of age restrictions against a clear problem definition, and against other options.
    - Other jurisdictions' regulatory approaches to online harm, including age restrictions, should be considered, and the results of those approaches assessed.
    - The method of age verification should be determined before legislation for any ban is introduced. Knowing how age would be verified is essential to assessing whether the intended benefits of the ban are proportionate to the risks.
    - The method of age verification should incorporate the principles of privacy by design, including collecting as little personal information as possible and building in strong security protections.

11. It is important not to lose sight of the need for broader regulation of social media and other online platforms, to make them safer not only for young people but also for all New Zealanders. Online platforms must be held accountable for designing their products and services in a way that safeguards young people's rights and interests. With regard to privacy, one way of helping to hold platforms to account would be to strengthen the tools and powers available to me under the Privacy Act. In particular, I recommend three key reforms to the Privacy Act:

    - a 'right to erasure', which would empower individuals to ask organisations to delete their personal information and set out when organisations must do so
    - a power for the Privacy Commissioner to impose substantial civil penalties for breaches of the Privacy Act
    - an 'accountability principle' that requires organisations to be able to demonstrate the purposes for which they are collecting personal information and how they will safely manage the information.

A privacy perspective on young people and online harms

12. The online world provides many benefits to young people,[1] including opportunities for social connection, exploring interests and education (including the development of digital skills and awareness). However, these benefits need to be balanced against risks children are exposed to online, including risks to their privacy. I am therefore pleased that the Committee is undertaking a broad inquiry into the harms young people encounter online, and how these can be addressed. I am also glad that the inquiry's terms of reference ask the Committee to consider online harms in the context of the benefits of online activity, and to evaluate the effectiveness and proportionality of potential responses to online harm.

13. It is important that our young people are kept as safe as possible from the types of harms identified in the inquiry's terms of reference. Among the harms that young people encounter online are breaches of their privacy and improper use of their personal information. Protecting young people against privacy harms is one focus of my submission. My Office is currently engaged in a project on children's and young people's privacy, looking at how young people's privacy can be better protected both online and offline. More information about this project is provided below.

14. My submission also addresses the importance of designing any interventions to protect young people online in a way that protects not only their privacy but the privacy of all New Zealanders. In particular, any proposed system of online age verification must be shown to be necessary and effective before it is introduced, and must be designed to capture as little personal information as possible.

15. Finally, my submission encourages the Committee to consider the online harms experienced by young people in the broader context of harms that people of all ages may encounter online, and the need for more effective regulation of online content, including through the Privacy Act.

Protecting young people's privacy online

16. Personal information is sacrosanct (or tapu) to the young person and whānau it is associated with. Because of the greater vulnerability of young people to harm, protections for their privacy are particularly important. Many young people are exposed to the online world before they fully understand the risks associated with online interactions. Young people's online activities often involve the collection, use and sharing of their personal information, which in turn can create risks to their privacy online. However, young people may be unaware of these risks, or of the ways in which their personal information is being used.

[1] I will follow the inquiry's terms of reference in using the term 'young people' to refer to children (tamariki) and young people (rangatahi).

17. These risks include:

- overcollection of young people's personal information by apps, websites and third parties
- apps or websites using young people's information in ways they have not authorised or are not aware of (such as targeted marketing, tracking, profiling or sharing of information with third parties)
- oversharing of information about or images of young people on social media by parents and others
- access to objectionable or otherwise age-inappropriate content
- online predators and scams, including those enabled by overcollection and reuse of personal information
- cybersecurity risks, including phishing, malware, and leaks or errors from badly secured systems
- cyberbullying.

18. Young people are also increasingly interacting with artificial intelligence (AI) chatbots and tools online. AI tools present new privacy risks and amplify old ones. Generative AI tools that are readily available online can collect, consume and use young people's personal information while also potentially exposing them to inappropriate content (responses to prompts). Use of generative AI platforms that mimic human interactions, such as conversational chatbots, may encourage young people to share personal information, creating risks that their information may be used in ways that are harmful to them, with no clarity on who is holding the information and what it might be used for.[2]

19. Young people's privacy, particularly in online environments, is a significant concern for New Zealanders. My Office commissions annual surveys of New Zealanders' opinions on privacy. The 2025 survey found that two out of every three New Zealanders are concerned about both the privacy of children, including when they use social media, and the management of personal information by social media companies more generally (67% and 63% respectively).

20. A recent survey of young people by Save the Children and Netsafe found that they are having positive experiences online, but also that they would like more support and tools to help them stay safe. Most of those surveyed wanted more control over the ads and content they see online, and a significant proportion wanted more privacy and control over what they share.[3]

---

[2] Tiffany Kwok and Christelle Tessono, *(Gen)eration AI: Safeguarding youth privacy in the age of generative artificial intelligence*, The Dais, Toronto Metropolitan University, Canada, 2025.
[3] Save the Children and Netsafe, *Report: Children and Online Safety in Aotearoa New Zealand*, June 2025.

Office of the Privacy Commissioner's children and young people's privacy project

21. Young people (rangatahi) are entitled to respect for their inherent dignity (or tapu), status (or mana) and well-being (or mauri). This means their human rights must be upheld, including their right to privacy. Young people in New Zealand have the same privacy rights as adults and can expect that their personal information will be respected and looked after by organisations. However, young people are more vulnerable to privacy harms, so they require additional care to ensure that their privacy is protected, especially online. For this reason, and in response to public concerns about young people's privacy, my Office launched a children and young people's privacy project in 2023.

22. This project started by consulting with government agencies, professionals who work with young people (such as teachers, doctors and nurses), and non-governmental organisations who advocate for young people. We asked them for their thoughts on how to improve young people's privacy in New Zealand, and received 113 responses. In April 2024, we released a report on the themes and messages we heard in this consultation.[4]

23. One of three key themes that emerged from our consultation was concern about young people's use of social media and the risks of the online environment. Particular concerns identified in responses included:

    - parents posting images of or information about their children on social media
    - how social media companies collect and use young people's data
    - the risk of bullying
    - content (including photos, comments, and posts) being immortalised on social media
    - young people's social media data being shared with or used by third parties.

24. My Office will now be focusing on providing guidance and educational material in relation to young people's privacy rights and protections. We have produced posters about protecting young people's privacy online, and guidance about photography and filming of young people, including about sharing images online. The photography guidance notes that, as well as risks such as bullying, identity theft and exploitation, sharing images online can lead to unwanted attention or intrusion into a young person's privacy, or affect education or job opportunities later in life. Further guidance, including detailed privacy guidance for the education sector, will be released later in the year.

25. Guidance for young people and their parents and guardians can help to inform and empower them to take privacy-protective actions. However, there is also an important role for the law in protecting young people from privacy risks and other online harms. The Privacy Act applies to young people, but for the most part does not provide additional protections over and above those that apply to all New Zealanders. However,

[4] Office of the Privacy Commissioner, *Safeguarding Children and Young People's Privacy in New Zealand*, April 2024.

the Act does require organisations to take extra care when collecting information about children and young people.[5]

26. I outline later in this submission some law reforms that I believe would help to protect the privacy of young people.

Proposals to restrict young people's access to online content

27. Before discussing other law reform options, I want to address proposals to ban young people from accessing social media platforms or the internet more generally. As the Committee will know, the Australian Government has amended the Online Safety Act 2021 to prevent children under 16 from having accounts on age-restricted social media platforms, with the new requirements coming into effect in December 2025. Other jurisdictions have also explored or attempted to implement restrictions on young people's access to the internet.[6] In New Zealand, a proposed Member's Bill in the name of Catherine Wedd, the Social Media (Age-Restricted Users) Bill, would require social media platforms designated by regulations as age-restricted platforms to take all reasonable steps to prevent people under the age of 16 from being account-holders with such platforms.[7]

28. I recognise that there is significant public support for banning young people from accessing online platforms where they could encounter harms. Respondents to my Office's stakeholder survey overwhelmingly supported minimum age requirements for using social media.[8] Many of the young people surveyed by Save the Children and Netsafe also supported age-related restrictions on access to online content, although very few supported a blanket ban on access to social media.[9]

29. Despite evidence of public support, a ban on young people accessing social media platforms or the wider internet would carry significant privacy and other risks. I therefore cannot support such a ban unless a robust policy case can be made for it. To date, I have not seen such a case. I advocate taking a considered approach; New Zealand should learn from observing how overseas regulations work in practice, including how technical issues and administrative burdens are managed. Public support for social media age limits may shift as these issues play out and people build an understanding of the tradeoffs involved, including the need for adults to verify their age as discussed below.

---

[5] Privacy Act 2020, s 22, information privacy principle 4(b): an agency must take account of age when assessing whether the manner in which they collect personal information from children or young people would be unfair or unreasonably intrusive.
[6] Lisa M. Given, 'Other countries have struggled to control how kids access the internet. What can Australia learn?', *The Conversation,* 27 June 2024.
[7] Social Media (Age-Restricted Users) Bill, cl 7.
[8] Office of the Privacy Commissioner, *Safeguarding Children and Young People's Privacy in New Zealand*, April 2024, p 14.
[9] Save the Children and Netsafe, *Report: Children and Online Safety in Aotearoa New Zealand*, June 2025, pp 14-15.

30. From a privacy perspective, the main concern about banning young people from accessing online platforms or content is the means by which people's ages will be verified. I provide more information about this issue below.

31. In addition, a blanket ban may result in young people seeking workarounds to access content, which could leave them exposed to online environments with few or no child-centred privacy and safety controls. It could also deprive young people of the opportunity to learn, under adult supervision, how to access and use social media and other platforms safely and appropriately. Young people are growing up in a digital world, and we need to ensure they are supported to become informed and competent digital citizens. Part of this education is understanding the online risks, being able to identify them, and knowing how to report them safely. A ban is unlikely to support the development of these skills.

32. Restricting young people from online platforms also does nothing to stop parents or other adults from sharing personal information about them online. 'Sharenting' (parents or guardians sharing images or sensitive information about their children online) can create a digital footprint for young people that they have no control over, and may create risks to young people's safety and wellbeing. The role of parents, whānau and young people themselves in deciding what information about young people to share online requires careful consideration.

Age verification

33. Banning under-16-year-olds from online platforms would require steps to verify the age of *all* users. Age verification, in turn, would require the collection of personal information from all users, to establish that they are aged 16 or over.[10] Unlike offline age verification, which commonly requires only that a person show identification such as a driver licence, online verification generally involves private companies collecting and storing large amounts of personal information about individuals.

34. As US legal academic Eric Goldman explains:

> compared to the often benign process of authenticating age offline, doing age authentication online … imposes substantial harms on everyone – including, counterproductively, the minors that the laws are intended to protect. Online age authentication exposes minors (and adults) to heightened privacy and security risks. Furthermore, the online authentication process acts as a technical barrier to reader access that will dissuade readers from navigating around the Internet.[11]

35. Goldman goes on to explain the privacy and security risks involved in online age verification, which:

> seeks to ascertain an important and immutable personal attribute of a person. Many people consider their age to be sensitive information, and the process of figuring out

---

[10] Matt Burgess and Lily Hay Newman, 'The Age-checked Internet has Arrived', *Wired*, 25 July 2025.
[11] Eric Goldman, 'The "Segregate-and-Suppress" Approach to Regulating Child Safety Online', *Stanford Technology Law Journal*, vol 173, 2025, p 177.

> a person's age inevitably involves the disclosure of additional private information beyond age, some of it highly sensitive. Thus, requiring minors to disclose their age always invades their privacy. As the California Privacy Protection Agency staff noted, 'there is currently no privacy-protective way to determine whether a consumer is a child.' The leading age authentication methods, document review and visual inspections, each require readers to disclose highly sensitive information beyond their age, namely the information displayed on a government ID or the reader's appearance for biometric scanning. …
>
> The disclosure of highly sensitive authentication data exposes readers – including minors – to substantial information security risks, including identity theft, extortion and blackmail, financial fraud, more tailored commercial pitches, and data profiling.[12]

36. Australia has been undertaking a trial of age assurance technology ahead of the ban on under-16 access to social media coming into force. While a preliminary finding of the trial is that 'Age assurance can be done in Australia and can be private, robust and effective', specific data is not yet available, and privacy and technology experts have expressed concern about some of the preliminary findings.[13] The final report on the trial is due later this year.

37. One way to check an individual's age is to verify against an authoritative source, such as a government-issued identity document, or credit card or banking information. Collecting identity information about every user of the internet, or of social media platforms, in New Zealand would create significant risks of over-collection of personal information and the creation of 'honeypots' of identity data that could be stolen and used by fraudsters and identity thieves.

38. Facial analysis to determine an individual's approximate age is another possible form of age verification. Biometric information such as a person's facial features is inherently sensitive personal information, because it cannot easily be changed and is intimately tied to an individual's identity. For Māori, such information is also commonly regarded as tapu and is connected to whakapapa. Because of the sensitivity of biometric information, my Office has been developing a biometrics code of practice under the Privacy Act, and I expect to issue a final version of this code soon. It is particularly important to ensure that any collection and use of biometric information is necessary and proportionate. I would expect to see careful analysis of the options before any proposal to use biometrics for age verification is implemented.

39. Another concern about online age verification is the potential for inaccuracy. Facial scanning for age detection raises particular accuracy concerns. While biometric age detection continues to improve, it appears that it is not yet reliable enough to use as evidence of age for the purpose of controlling online access. Trials of age detection

---

[12] Ibid., pp 202-203, 204.
[13] Age Assurance Technology Trial, news release, 20 June 2025; Simon Sharwood, 'Australia Finds Age Detection Tech has Many Flaws but Will Work', *The Register*, 20 June 2025.

technology on high school students in Australia found that the technology could only estimate their ages to within an 18-month range in 85% of cases.[14]

40. Having noted these risks, I recognise that identity and age verification technologies are continually advancing. It may well be possible, or become possible in future, to find a solution which simply verifies that a person is, or is not, aged 16 or over, without collecting other information about the person. The Digital Identity Services Trust Framework is a legislatively-mandated framework for safely sharing information in a digital form. If an age verification system is to be developed, the option of integrating it into this framework should be seriously explored.

41. I am aware that age verification requirements have been included in the recently-introduced Online Casino Gambling Bill. I will be considering my position on that Bill separately, but if age verification is introduced through that Bill, it should not be considered a precedent for the broader introduction of online age verification. That Bill deals with access to a very specific and limited set of online platforms (online casino gambling sites), and the proposed age verification requirement addresses quite specific risks of young people engaging in harmful gambling. This is very different from requiring age verification for a wide range of commonly-used platforms, in order to address a broad and diffuse set of harms.

42. If an age-based ban on access to online platforms were to be introduced in future, two things are crucial:

    - The method of age verification should be determined *before* legislation for any ban is introduced. Knowing how age would be verified is essential to assessing whether the intended benefits of the ban are proportionate to the privacy and other risks.
    - The method of age verification should incorporate the principles of privacy by design, including collecting as little personal information as possible and building in strong security protections.

Better protections from online harm are needed

43. Young people face particular risks and have additional vulnerabilities in online spaces, compared to adults. Nonetheless, all users of the internet are exposed to online harms. There are steps we can all take to protect ourselves, but we also need effective regulation to ensure that online environments are as safe as can reasonably be expected. While it is important to ensure that young people are safe online, we must not lose sight of the bigger picture of protecting all New Zealanders from the most harmful content and behaviours online. That includes harms from systems that fail to keep our information secure, exposing young people and other New Zealanders to cybercrimes and data breaches.

---

[14] 'Six Months Out from Teen Social Media Ban, Age-checking Tech Mistakes Kids for 37-year-olds', ABC News, 19 June 2025.

44. Some aspects of online content and behaviour are regulated under the Privacy Act and other legislation, but there is no overarching or joined-up regulatory framework to keep people safe online. The question of how to respond effectively and proportionately to online harms needs to be addressed. Other countries are also grappling with this challenge, and New Zealand has an opportunity to learn from their experiences.[15]

45. With regard to protections for young people in particular, online platforms must be held accountable for designing their products and services in a way that safeguards young people's rights and interests. The focus should be on making the platforms safe, not on limiting young people's access to them. I direct the Committee's attention to the work of the 5Rights Foundation, an international non-government organisation working with and for children for a rights-respecting digital world. I agree with the Foundation that 'Children's rights and needs must be at the heart of digital design and development. Tech companies must be held accountable for ensuring their products and services cater for children and young people by design and default.'

46. An example of a regulatory approach that focuses on the design of online services is the UK's Age-appropriate Design Code, a code of practice issued by the Information Commissioner's Office under the UK's equivalent of the Privacy Act. To comply with the code, online services need to think about such things as:

    - mapping what personal data they collect from UK children
    - considering the age of the people who visit their website, download their app or play their game
    - switching off geolocation services that track where their visitors are
    - not using nudge techniques to encourage children to provide more personal data
    - providing a high level of privacy by default.

    The 5Rights Foundation has also recently issued a Children and AI Design Code, aimed at ensuring children's needs are prioritised by design and default when AI systems are built and deployed.

47. The Privacy Commissioner can issue privacy codes of practice under the Privacy Act. However, my code-making power can only be used to modify the existing information privacy principles in the Act in relation to particular types of information, activities or sectors. It could not be used to introduce broader requirements for age-appropriate design of online platforms. Further, any such code of practice is unlikely to fully realise the intended benefits of protecting young people's privacy without the stronger enforcement tools and powers discussed below.

---

[15] Examples of regulatory approaches in other jurisdictions include the European Union's Digital Services Act, the United Kingdom's Online Safety Act, Ireland's Online Safety and Media Regulation Act, Singapore's Online Safety (Miscellaneous Amendments) Act, and Australia's Online Safety Act. Such legislation is generally accompanied by codes of practice and guidance.

Privacy Act reform can help protect young people online

48. I will limit my recommendations for specific law reforms to those that can be implemented through amendments to the Privacy Act. The reforms discussed below would help to protect young people, but would also better protect all New Zealanders from privacy harms online. They would provide New Zealanders with stronger privacy rights, and my Office with more effective tools to enforce those rights.

A right to have information deleted

49. With the increasing digitisation of modern economies, many of our international partners have established new privacy rights for their citizens, such as a 'right to erasure'. Rights to erasure provide individuals with the ability to ask organisations to delete their personal information and set out when organisations must do so. The European Union first introduced this important right in 2018 and California in 2020. The Australian Government has agreed in principle to establish a right to erasure.

50. Many submissions to my Office's survey of stakeholders about safeguarding young people's privacy supported a right to erasure. They noted in particular the risks of young people's information being collected and misused by social media companies, or being shared inappropriately online by the young people themselves or by others. Sixty-nine per cent of survey respondents said that they wanted the right for children to ask for their information to be deleted from social media.[16]

51. Amending the Privacy Act to provide individuals, including young people, with a right to erasure would empower them to go directly to the organisations concerned to seek to have their information removed from online platforms. My Office can then provide guidance and act on complaints and compliance issues that arise.

Stronger enforcement tools

52. Resolving privacy breaches and respecting the dignity, status and wellbeing of those affected requires action to provide restitution and prevent similar breaches from occurring in future. At present, the maximum penalty under the Privacy Act is a fine not exceeding $10,000, and this can only occur in limited circumstances. My Office's investigations into privacy breaches have revealed that some organisations do not care about privacy as they know there are no significant financial penalties.

53. In contrast, other countries are steadily introducing very high financial penalty regimes, reflecting the digital age we live in. For example, in 2022 Australia strengthened its civil penalty regime so that a serious or repeated interference with privacy has a maximum penalty of AUD$50,000,000, or three times the value of the benefit obtained directly or indirectly. This discrepancy between the penalties available in New Zealand and in other jurisdictions is particularly significant when considering privacy breaches by online

[16] Office of the Privacy Commissioner, *Safeguarding Children and Young People's Privacy in New Zealand*, April 2024, p 12.

platforms that operate internationally. Such platforms are likely to be more responsive to overseas regulators who can impose higher penalties.

54. I believe a power for the Privacy Commissioner to impose substantial civil penalties on organisations that breach the Privacy Act would create a stronger incentive for organisations to take privacy, including young people's privacy, seriously. Civil penalties offer a discretionary and flexible tool and they can be used to respond to a significant breach or non-compliance that puts personal information at risk. Civil penalties provide a means to punish serious breaches, including repeat offending. They act as an incentive to encourage agencies to cooperate and to mitigate the risk of harm, and strengthen the position of those within organisations who are working to ensure that policies, procedures and investment decisions support good privacy practice.

Greater transparency about organisations' privacy practices

55. My Office's experience has shown that many organisations have not considered how they will safely manage personal information. While the Privacy Act has requirements that an organisation must meet (such as maintaining appropriate security safeguards), there is no requirement for anything to be documented. This creates difficult situations for my Office if non-compliant organisations have no policies, procedures or privacy documentation.

56. Many countries and international privacy frameworks have an 'accountability principle' that requires organisations to be able to demonstrate the purposes for which they are collecting personal information and how they will safely manage the information. Including such a principle in the Privacy Act would help to make it clearer when an organisation's handling of personal information, including information about young people, is in breach of the Act. It would help to hold online platforms that collect information about young people accountable by requiring them to demonstrate their compliance with the Privacy Act to the Privacy Commissioner on request.

Conclusion

57. This submission has brought a privacy focus to the issues under consideration by the Committee. The Committee will no doubt hear from a wide range of individuals and organisations, bringing differing perspectives and expertise to the discussion. These are challenging issues, with no easy answers, and I look forward to hearing these diverse perspectives. I strongly encourage the Committee, in its hearings and deliberations, to take an approach that focuses on protecting human rights, including the right to privacy, and to listen carefully to the views of young people themselves. To date, discussion of young people and online harm has been dominated by adults, and it is important that we hear from young people directly about the benefits and risks of being online, as well as their ideas for ways of addressing the risks.

58. I trust my comments are of use to the Committee. I am happy to appear before the Committee if that would be of assistance.

Michael Webster
Privacy Commissioner

30 July 2025