YOUTH PRIVACY IN AUSTRALIA

Insights from National Policy Dialogues

NOVEMBER 2025

FUTURE OF PRIVACY FORUM | aarnet

AUTHORS

Bailey Sanchez
Deputy Director, U.S. Legislation, Future of Privacy Forum

Jordan Wrigley
Data and Policy Analyst for Health & Wellness, Future of Privacy Forum

---

AARNet: Australian Academic and Research Network is Australia's national research and education network, owned by the universities and CSIRO, and operated as a not-for-profit company dedicated to advancing knowledge and discovery. For over 30 years, AARNet has provided trusted telecommunications, collaboration, and cybersecurity services, all designed to meet the unique and changing needs of research and education.

AARNet works closely with the research and education sector, industry, and government to promote a safe and secure internet environment, fostering innovation while protecting the integrity of Australia's digital infrastructure.

Learn more at arnet.edu.au

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

TABLE OF CONTENTS

I. INTRODUCTION

Throughout the fall of 2024, the Future of Privacy Forum (FPF), in partnership with the Australian Academic and Research Network (AARNet) and Australian Strategic Policy Institute (ASPI), convened a series of three expert panel discussions across Australia exploring the intersection of privacy, security, and online safety for young people.

This event series built on the success of a fall 2023 one-day event that FPF hosted on privacy, safety, and security regarding industry standards promulgated by the Office of the eSafety Commissioner (eSafety). These discussions took place in Sydney, Melbourne, and Canberra, and brought together leading academics, government representatives, industry voices, and civil society organizations.

The discussions provide insight into the Australian approach to improving online experiences for young people through law and regulation, policy, and education. By bringing together experts across disciplines, the event series aimed to bridge divides between privacy, security, and safety conversations, and surface key tensions and opportunities for future work.

This report summarizes key themes that emerged across these conversations for policymakers to consider as they develop forward-looking policies that support young people's wellbeing and rights online.

II. BACKGROUND

Australia has embarked on several regulatory initiatives focused on protecting children and teens online. For instance, on November 29, 2024, the Australian Government passed a first tranche of updates to the Privacy Act, with the possibility of more amendments in the future. The first passed amendments included a mandate for the Office of the Australian Information Commissioner to develop a Children's Online Privacy Code, which will specify how online services accessed by children must comply with the Australian Privacy Principles. Perhaps most significantly, just after this event series concluded, the Australian Government also passed the novel Online Safety Amendment (Social Media Minimum Age) Bill on the same day as the first tranche of privacy amendments. This bill amended the existing Online Safety Act to require certain social media platform providers to take measures to prevent children below the age of 16 from having accounts on age-restricted platforms. eSafety now works towards implementation of the prohibition, which will take effect by December 10, 2025.

III. KEY THEMES & TAKEAWAYS

1. Bridging Divides Between Privacy, Safety, and Security

A foundational insight from the event series was the critical need to break down silos between the fields of privacy, safety, and security. These areas, though interconnected, are often approached through separate policy frameworks or even viewed in tension with one another. For instance, proposals to increase online safety can sometimes undermine privacy, while security initiatives may inadvertently diminish user autonomy.

At each event, speakers emphasized the importance of interdisciplinary dialogue to avoid these tradeoffs. One expert observed, *"Young people are not just data subjects or risk profiles—they are whole people navigating complex environments. If we improve safety but degrade their privacy, we haven't truly protected them."* Another noted that gains in one area can and should reinforce others when thoughtfully approached: *"There are creative ways to protect against abuse, support safety, and still uphold encryption and privacy standards. It's not always either-or."*

This integrated approach is particularly critical given that failures in any of these domains disproportionately affect young users, whose digital lives are shaped early and have long-term consequences.

2. Learning from Governing Past Technologies to Inform Emerging Ones

A recurring point across events was that today's policy decisions about AI, algorithmic systems, and emerging technologies must be informed by lessons learned from regulating prior technologies—especially social media. Several experts stressed that generative AI, while novel in form, often amplifies well-known harms rather than creating entirely new ones.

One framework presented at the events asked: *Is the harm new? A magnified prior harm? Or a misunderstood repeat?* This model encourages policymakers to distinguish hype from harm and to apply established regulatory principles where they still hold relevance.

For example, some long standing concerns with social media platforms, including data collection practices and opaque algorithmic decision making, are now manifesting in AI-powered educational and entertainment tools aimed at children. *"We don't need to reinvent the wheel,"* one participant said. *"We need to recognize patterns and improve on how we've handled them before."* The discussion made clear that the window of opportunity to shape these systems responsibly is narrow—and must be seized now.

3. Encryption, Identity, and the Unintended Consequences of Online Safety Policy

While every participant agreed on the importance of safeguarding young people with age-appropriate protections from online harm, there was concern that some well-intentioned interventions could create significant risks. In particular, proposals requiring age verification or weakening encryption were flagged as negatively impacting both privacy and security.

Many stakeholders were critical of efforts to mandate age verification across online services without appropriate privacy safeguards, noting the implications for youth privacy and for vulnerable groups more broadly. As one panelist stated, *"If you make identity the price of admission online, you exclude and endanger whole communities."* End-to-end encryption was another flashpoint. Though sometimes framed as a barrier to law enforcement, it was repeatedly described as a critical tool for protecting users from surveillance, abuse, and data breaches.

Experts encouraged policy approaches that balance law enforcement needs with robust safeguards for privacy. As one speaker cautioned, *"We cannot protect children by building a less secure internet for everyone."*

4. Education as a Shared and Evolving Responsibility

Education, both formal and informal, was acknowledged as an essential layer in protecting young people, though not a standalone solution. Participants agreed that young people must be equipped to make informed decisions online, and that digital literacy must be tailored to different developmental stages.

Importantly, speakers highlighted the everyday, informal learning that takes place as children explore the internet. *"Kids are teaching themselves digital resilience in real time,"* said one participant. But this does not absolve stakeholders of responsibility. Parents, educators, platforms, and regulators all have a role to play.

However, there was strong agreement that schools should not bear the burden alone. *"We've reached the limit of what educators can do on their own,"* a panelist warned. Policy must support rather than overextend educators and should integrate education efforts with industry and government actions. Education must also reach adults, including parents and policymakers, so they can keep pace with the changing landscape.

5. Youth Agency: Engaging Youth as Stakeholders, Not Just Beneficiaries

Rather than designing policy "for" young people, events stressed the value of designing "with" them. Many discussions returned to the theme of youth agency—how young people experience trust online, what autonomy they have (or are denied), and how digital systems either respect or undermine their choices.

As one participant put it, *"We protect young people best when we treat them as partners in their own safety, not just as passive recipients of protection."* This requires meaningful engagement, not tokenism. Several speakers called for more youth consultation in regulatory and platform decision-making processes, pointing to successful youth-led digital rights movements globally.

The concept of "developmental appropriateness" also featured prominently. Young people's needs vary dramatically by age, context, and individual capacity. One size rarely fits all, and good policy must accommodate complexity and nuance.

6. AI: The Dual-Use Dilemma

The Melbourne event explored how generative AI introduces both profound opportunities and profound risks for young people. On the one hand, AI-powered tools can personalize learning, support creativity, and foster new modes of expression. On the other, they can be used to spread misinformation, impersonate individuals, or even generate harmful and exploitative content.

A recurring concern was the use of AI to produce synthetic sexual abuse material (including deepfake child sexual exploitation), which several panelists warned is an urgent and growing problem. However, many also emphasized the risk of moral panic leading to reactive or overbroad regulation. Instead, discussions pointed to the need for strong governance frameworks that include transparency, auditability, and child rights impact assessments.

"We don't want to ban the future. But we do want to shape it," summarized one speaker. Many called for AI regulation that builds on existing child-focused data protection laws while adapting to the unique risks AI poses.

7. Trust as an Outcome of Good Policy and Design

Ultimately, many conversations circled back to trust and how it is built and sustained. One participant distinguished between "trust" and "trustworthiness" as the act of earning youth and parent trust rather than assuming or requesting it. Young people's willingness to engage online depends on whether they feel safe and respected in digital spaces. While trustworthiness may be supported by policy, participants noted trust cannot just be legislated into existence; it must be earned through transparency, consistency, and fairness.

"Secure online spaces can provide an opportunity for young people to learn more about the world, exercise creativity, and discover more about themselves."

Design choices—like clear privacy settings, minimal data collection, and visible safety features—can reinforce that trust. So too can policies that respect user rights and provide accessible redress mechanisms.

As one participant concluded: *"When we prioritize trust, we get privacy, safety, and security as a package—not a compromise."*

IV. CONCLUSION

This event series made clear that young Australians wish for a digital ecosystem that is not only safe and secure but also respectful of their privacy and autonomy. As Australia prepares to implement reforms to its Privacy Act and develop child-centered policies and codes, the insights from these discussions offer important guidance.

To create a future where young people can thrive online, policymakers should aim to:

- Treat privacy, safety, and security as interconnected,
- Avoid zero-sum approaches that trade one value for another,
- Incorporate formal and informal education, but not rely on it alone,
- Protect encryption and privacy-enhancing technologies,
- Meaningfully include youth voices, and
- Design policy and technology in ways that build trust and resilience.

The Future of Privacy Forum and its partners thank all participants for their insights and collaboration. We look forward to supporting continued work in this space to ensure a safer and more trustworthy digital world for the next generation.

EVENT DESCRIPTIONS & SPEAKERS

EVENT ONE

Looking Toward the Future: Building a Safe, Secure, and Private Internet for Everyone

Held September 4, 2024 in Sydney

As nations globally align their regulatory frameworks to address these topics, this panel will provide critical insights into the Australian approach to enhancing online experiences for young people, including through law and regulation, policy, and education.

Australia is poised at the cutting edge of regulatory advancements in online privacy and security, yet significant milestones lie ahead. Anticipated developments include forthcoming updates to the Privacy Act, new industry guidelines from eSafety, and the introduction of a Children's Online Privacy Code by the Australian Government. These initiatives are instrumental in crafting a secure and empowering digital environment for the youth, balancing the imperatives of privacy, safety, and security. Additionally, educators not only help young people navigate digital landscapes safely but also play a crucial part in fostering digital literacy and responsible online behavior. By integrating education with policy efforts, we can better equip the younger generation to understand and manage their privacy and security in an evolving digital world.

**Note: This event was formatted as a roundtable discussion of 20 leaders from government, industry, academia, and education. Opening remarks were delivered by Dr. Andrew Charlton MP, Special Envoy for Cyber Sec'y & Digital Resilience. The discussion was moderated by John Verdi, Senior Vice President for Policy at the Future of Privacy Forum and Jodi Roker, Director, Government Affairs & Partnerships at AARNet.*

EVENT TWO

The Impact of Generative AI on Kids' Privacy, Safety, and Security

Held October 15, 2024 in Melbourne

AI—Artificial Intelligence—has been around for years, but with the recent widespread release of consumer-facing AI tools that can generate text, images, audio, and video, understanding the technology's risks and benefits has never been more important. When it comes to young people, generative AI has the potential to allow for new creative outlets, improve independent learning, and provide for more personalized education. However, it also has the potential to exacerbate some of the harms already experienced online, such as harassment, bullying, and the development of AI-generated child sexual exploitation material (CSEM).

This session will focus on potential risks and benefits related to children's use of the growing suite of generative AI tools and methods for combatting existing and emerging harms to young people online, including the impact of the upcoming updates to Australia's Privacy Act and the ongoing work of various Australian digital platform regulators on generative AI and AI governance.

KEYNOTE SPEAKER

Mr. Peter Khalil, MP Chair of Parliamentary Joint Committee on Intelligence and Security, Member for Wills

SPEAKERS

Moderator: Dr. John Coyne, Head of the Northern Australia Strategic Policy Centre and Head of Strategic Policing and Law Enforcement, ASPI

PANELISTS

- Associate Professor Campbell Wilson, Co-director of the Ai for Law Enforcement and Community Safety (AiLECS) Lab, Monash University
- Dr. Jessica Lake, Senior Lecturer, University of Melbourne
- Dr. Shaanam Cohney, Senior Lecturer in Cyber Security Computing and Information Systems, University of Melbourne
- Bailey Sanchez, Deputy Director, U.S. Legislation, Future of Privacy Forum

EVENT THREE

Navigating Digital Safety: Exploring Security and Trust in Online Spaces for Young Australians

Held November 27, 2024 in Canberra

As technology evolves, so do the challenges of privacy, internet security, and online safety. As users of online platforms, young Australians are exposed to varied and increasing risks, including risks to their personal data privacy. Online spaces are also increasingly threatened by criminal and state-backed actors, and challenges to social cohesion. In our current digital context, what does it truly mean to be secure online, and how can we create a safer digital environment?

This event will focus on digital safety through the lens of online security and safety as well as national security and law enforcement, with a strong emphasis on engaging young people and government representatives. For the panel discussion, FPF, AARNet, and ASPI will bring together experts to discuss what it means to be secure online, current and emerging security challenges, and the ways that secure online spaces can provide an opportunity for young people to learn more about the world, exercise creativity, and discover more about themselves.

The panel will discuss the dimensions to internet security, both personal and corporate, how security ties into notions of privacy and safety, as well as challenges certain security technologies may pose to law enforcement investigations. In addition, panellists will be asked to consider a range of policy proposals that governments are proposing to regulate data – including updates to the Privacy Act, proposals to authenticate all internet users, and age verification for certain products or services—and the impact those proposals may have on trust and security.

SPEAKERS

Moderator: Amie Stepanovich, Future of Privacy Forum

PANELISTS

- Huon Curtis, PhD, Digital Resilience Network
- Ben Au, Manager, ANZ Public Policy, Snap Inc.
- Mandy Ross, Director, Strategic Partnerships Defence, Monash University
- Dr. John Coyne, Head of the Northern Australia Strategic Policy Centre and Head of Strategic Policing and Law Enforcement, ASPI

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005 FPF.ORG | info@fpf.org