

Smartphone sharing in couples: Agenda for Future Action

Molly Dragiewicz, Jeffrey Ackerman & Marianne Haaland
2025

Recommendation One: Expand smartphone cybersecurity options

- Binary all-or-nothing access models are inadequate for everyday smartphone use.
- Safety by design principles should apply to smartphones and mobile applications.
- Make secure sharing settings the default on smartphones.
- Design devices and applications to facilitate easy adjustments to sharing permissions as needed.

Recommendation Two: Integrate intimate threats into cybersecurity models

- While domestic and family violence has been integrated into criminology, law, and policing in Australia, cybercrime frameworks have yet to recognise intimate threats as core concerns for cybersecurity.
- Integrating insights from research on domestic, family, and gender-based violence and how consumers use technology into State and industry cybersecurity frameworks can yield more robust models to address the full spectrum of threats.
- Acknowledge and investigate why consumers share smartphones so that positive social functions can be accommodated alongside harm and risk mitigation.

Recommendation Three: Promote informed consent for smartphone sharing

- Any technology or technology behaviour can be used to promote or threaten security and well-being.
- The context of technology behaviours is what gives them their meaning.
- Open communication can help reduce potential conflicts and risks associated with device sharing in couples.
- While communication about expectations for sharing cannot prevent technology-facilitated abuse, it can raise awareness of factors to consider in the future if the nature of the relationship changes.