



Beyond Takedown: Effective Containment of Reposted Harmful Material

Consultation on the *Exposure Draft Online Safety Amendment
(Digital Duty of Care) Bill 2026* (Cth)

**Submitted to the Department of Infrastructure, Transport, Regional Development,
Communications, Sport and the Arts**

22 September 2026

Prepared by

Mr Alfred Muscat

Associate Research Fellow | Social Cyber Institute

Approved by

Dr Greg Austin

Co-founder and Research Director of the Social Cyber Institute

The views of this submission do not necessarily reflect the views of the Social Cyber Institute.

The proposed *Online Safety Amendment (Digital Duty of Care) Bill 2026* represents an important shift in Australian online-safety regulation. Its central premise is correct: online-service providers should not be permitted to wait until serious harm has occurred and then respond only to individual complaints. They should be required to identify foreseeable risks, design safer services and take effective measures to prevent harm. This preventative approach is particularly important for children, whose privacy, dignity and long-term welfare can be profoundly affected by the circulation of harmful material.

The proposed reduction of several removal periods from 48 hours to 24 hours is therefore welcome. In cases involving cyberbullying, sexualised deepfakes, non-consensual intimate imagery or threats of violence, every hour of continued availability can materially increase the harm. Content can be downloaded, copied, indexed, recommended and redistributed to a large audience well before the expiry of a 24-hour period.

The difficulty, however, is not merely that the proposed timeframe remains too long for the most serious cases. The larger problem is that the removal framework continues to treat harmful material as though it were a static item located at a single URL. That does not reflect the nature of modern online dissemination.

The exposure draft partly recognises this problem. Proposed subsections 65(2C)–(2E), together with equivalent provisions applying to other removal schemes, allow the eSafety Commissioner to issue a further removal notice without requiring a new complaint where material subject to an earlier notice is reposted within six months. The definition of “reposted” is appropriately broad. It includes material that has been shortened, extended, cropped, reproduced as a screenshot or accompanied by altered text, dialogue or commentary.

This is a meaningful improvement, but it does not adequately address the underlying problem. It streamlines the issue of another notice after a repost has been found; it does not impose a clear obligation on the provider to prevent the repost or contain its further dissemination. The victim or Commissioner must still discover the new copy, establish that it is a repost and commence another regulatory response. By then, the material may have migrated to multiple accounts, groups, search results and services.

For a child, repeated circulation is not a collection of separate incidents. It is one continuing invasion of privacy and dignity. Each repost renews the exposure, expands the audience and further deprives the child of control over their image, identity and personal information. A framework that requires a child or their family to repeatedly search for and report substantially identical copies risks transferring the burden of platform failure onto the person the legislation is intended to protect.

That burden can itself be harmful. Requiring a child to continually revisit abusive or sexualised material in order to secure its removal may compound distress and undermine recovery. The law should not make effective protection dependent on the persistence, technological literacy or financial resources of the affected child and their family.

The Bill should therefore impose an obligation of effective containment, rather than treating compliance as complete when a notified post or URL has been removed. Once a provider has actual knowledge that material involving a child falls within a prescribed category of serious harm, the provider should be required, so far as reasonably practicable, to:

- remove or disable access to all known copies and materially equivalent variants on its service;
- use proportionate measures to prevent the same material from being re-uploaded for a defined period;
- prevent recommender systems, search functions, trending systems and engagement features from amplifying it;
- identify accounts engaged in coordinated or repeated redistribution;
- preserve necessary evidence securely for regulatory or law-enforcement purposes; and
- provide the affected child or their representative with one continuing case reference, rather than requiring a new complaint for every subsequent copy.

These obligations should extend beyond exact file matches. Minor alterations, including cropping, mirroring, filters, captions, compression and screenshots are routinely used to evade automated detection. The statutory concept of reposting already recognises this reality. The practical obligations imposed on providers should do the same.

The Bill should also distinguish between ordinary complaints and acute child-safety cases. Twenty-four hours may be an appropriate maximum period for some categories of material, but it should not become a universal default. For child sexual abuse material, non-consensual intimate imagery involving a child, fake nude material depicting a child, credible threats and material creating an imminent risk of serious physical harm, providers should be required to act as soon as practicable, subject to a much shorter outer limit. A one-hour requirement following a verified notice would be appropriate for these exceptional categories.

The relevant period should commence when the provider receives a sufficiently particularised report, not when its internal processes formally classify or escalate the complaint. Otherwise, a platform could effectively control the statutory clock through its own administrative arrangements. Providers should also be required to acknowledge urgent reports immediately, preserve evidence and notify the complainant when effective containment measures have been implemented.

Cross-platform migration must also be addressed. Harmful material rarely remains confined to the service on which it first appeared. It may move rapidly from a social-media account to a messaging service, hosting site, search engine or generative-AI tool. The Commissioner should be empowered to operate a secure notification mechanism through which verified identifiers of prescribed child-harm material can be communicated to relevant services. Participating providers should then be required to assess whether the same material is present on, or being distributed through, their services.

Any such system must contain strong safeguards. Protecting children online cannot justify indiscriminate surveillance or unnecessary interference with private communications. Effective containment should be implemented through privacy-preserving technologies, strict access controls, limited retention periods, independent auditing and meaningful human review. Automated tools should assist in identifying previously confirmed harmful material and close variants; they should not become an unreviewable system for monitoring lawful expression.

Particular caution is required in relation to retention. A child's intimate or manipulated images should not become a permanent platform-held dataset merely because the child sought protection. Where perceptual hashes or other digital identifiers are used, the

underlying material should be retained only where necessary for evidence, review or legal proceedings, and then subject to secure storage, access limitations and mandatory deletion periods.

There should also be accessible review and correction mechanisms. Automated systems can make errors, and an incorrectly classified image could affect lawful family photographs, educational material, health information or legitimate journalism. Providers must therefore maintain processes through which affected users can seek prompt human review without weakening urgent protections for children.

The proposed reduction from 48 hours to 24 hours is a positive step, but speed alone will not resolve the problem. A modern online-safety regime must regulate the complete lifecycle of harmful material: uploading, recommendation, copying, alteration, indexing and redistribution. It must also recognise that the practical burden of repeated enforcement should fall on the services that design and control digital systems, not on children who have already suffered harm.

The proper measure of compliance is not whether one identified URL was removed within 24 hours. It is whether the provider took reasonable, proportionate and effective steps to stop a known harm from continuing.