Electronic Frontiers Australia Inc.
ABN: 35 050 159 188
W www.efa.org.au
E email@efa.org.au
@efa_oz

Executive Manager, Investigations
Office of the eSafety Commissioner
PO Box Q500
Queen Victoria Building NSW 1230

12 September 2021

By web form

Dear Executive Manager,

RE: Restricted Access System call for submissions

EFA welcomes the opportunity to comment on the proposal for a new Restricted Access System mechanism.

EFA's submission is contained in the following pages.

About EFA

Established in January 1994, EFA is a national, membership-based, not-for-profit organisation representing Internet users concerned with digital freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political, and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,

Justin Warren
Board Member
Electronic Frontiers Australia

Introduction

EFA has been responding to Australian government attempts to implement a society-wide Restricted Access System to limit access to online content for over two decades.[1] Despite the lack of success across time, governments remain undeterred in continuing to advocate for the same overbroad technical solutions to what are inherently social issues.

EFA believes this latest attempt to square the circle—at great cost in time and expense—is similarly doomed to fail.

This well-meaning, but misguided, effort once again provides a distraction from the challenging and serious work required to address the social issues that need to be addressed. And not only a distraction: it will also harm a great number of people who are already suffering, who are already pushed to the margins of society, and who—time and time again—ask to be included in decisions made about them, to be allowed to participate in building the systems they must work within, only to be rebuffed, ridiculed, and ignored.

And yet they keep trying.

EFA stands ready to work with the government when it decides it wants to tackle this complex and difficult challenge with the seriousness it deserves.

Summary of Recommendations

1. **EFA recommends that eSafety heeds the research that indicates that education and contextual support provides better child development outcomes than authoritarian ban-hammers.**
2. **EFA recommends that the responsibility for what material children are permitted to access should remain with their parents, guardians, and other responsible adults actively involved in their upbringing.**
3. **That the restricted access system determination explicitly takes into account the much broader scope of the *Online Safety Act* compared to the *Broadcasting Services Act*.**
4. **That any determination explicitly limits the requirement for a restricted access system to only adult content services and excludes general-purpose communications systems.**
5. **That the physical location of a customer should not be required in order to perform age verification checks.**
6. **That the identity of a customer should not be required in order to perform age verification checks.**

[1] 'ABA Consultation Paper - Restricted Access Systems - EFA Response' <https://www.efa.org.au/Publish/ABAresp9911.html>.

7. **EFA recommends that all communications of a given type should be subject to the same restrictions or lack thereof.**
8. **That the government should not attempt to mandate the creation of a separate "Children's Internet".**
9. **That parents, guardians, and similar responsible adults should be the arbiters of what the children in their care view on the Internet.**
10. **EFA recommends that the eSafety Commissioner does not repeat the same mistakes that others have made attempting to implement restricted access systems.**
11. **EFA recommends that certain classes of material should be explicitly exempted from restricted access systems, with penalties for incorrect censorship or removal.**
12. **EFA recommends that alternate, privacy-enhancing solutions to content access control are explored before enacting an age-verification system.**
13. **That the restricted access system declaration incorporates any changes resulting from the review of Australian classification regulation.**
14. **EFA recommends that the eSafety Commissioner refer all classification decisions to the Classification Board to ensure consistency of classification decisions.**
15. **EFA recommends that the protections from civil proceedings provided by s 221(2) and s 222 of the *Online Safety Act* should not apply if a decision is made without due care, diligence, and skill.**
16. **That the eSafety Commissioner set aside funds in a compensation scheme accessible by individuals and groups harmed by mistakes made by eSafety or those following eSafety's directions.**
17. **That the eSafety Commissioner explicitly details the expected number and magnitude of errors per year that it deems is acceptable.**
18. **That any protections from civil or criminal liability are only available if an entity acts with due care, skill, and diligence.**

Submission Detail

Our submission addresses the following broad areas:

- Nature of the alleged problem
- Changes since the *Broadcasting Services Act*[2]
- Technical feasibility
- Adverse consequences

Nature of the alleged problem

It is not currently illegal for people under the age of 18 to view pornography under Australian law.[3]

The purported goal of requiring restricted access systems is "to achieve a proportionate, effective and feasible age verification regime for the purposes of reducing the exposure of children and young people under 18 to online pornography in Australia."[4] It is not explained why "the exposure of children and young people under 18 to online pornography in Australia" is inherently harmful to the degree that age restriction systems are necessary. Research indicates that we should not conflate sexual content with risk.[5]

According to the Australian Institute of Family Studies "[p]arents tend to overestimate exposure to pornography for younger children and underestimate the extent of exposure for older children."[6] The AIFS stresses that "it's important to remember that children and young people are naturally curious about sexuality, and will seek out information about sex and relationships"[7] and provides a range of expert-recommended approaches to assisting children to develop mature and healthy attitudes to sex and relationships.

Indeed, there is a large and growing body of research that highlights that merely blocking access to content based on a clumsy age-based threshold is not in childrens' best interests, and that childrens' healthy sexual development requires a more nuanced and contextual approach.[8]

---

[2] *Broadcasting Services Act 1992*.
[3] While there are prohibitions on selling or displaying pornographic materials to minors, it is not illegal for a minor to merely possess or view pornographic materials.
[4] Office of the eSafety Commissioner, 'Restricted Access System Declaration Online Safety Act 2021 Discussion Paper' (Australian Government, August 2021) <https://www.esafety.gov.au/sites/default/files/2021-08/OSA%20-%20Restricted%20Access%20System%20discussion%20paper_0.pdf>.
[5] Susanna Paasonen, Kylie Jarrett and Ben Light, *NSFW: Sex, Humor, and Risk in Social Media* (MIT Press, 2019) ('*NSFW*').
[6] Australian Institute of Family Studies, 'The Effects of Pornography on Children and Young People', *Australian Institute of Family Studies* (Text, 7 December 2017) <https://aifs.gov.au/publications/effects-pornography-children-and-young-people-snapshot>.
[7] Monica Campo, 'Children and Young People's Exposure to Pornography', *Child Family Community Australia* (Text, 4 May 2016) <https://aifs.gov.au/cfca/2016/05/04/children-and-young-peoples-exposure-pornography>.
[8] Alan McKee et al, 'Healthy Sexual Development: A Multidisciplinary Framework for Research' (2010) 22(1) *International Journal of Sexual Health* 14 ('Healthy Sexual Development').

Simply banning anyone under the age of 18 from ever seeing a penis or a boob is a Puritanical attitude that is more suited to Victorian-era England than modern Australia.

Recommendation: EFA recommends that eSafety heeds the research that indicates that education and contextual support provides better child development outcomes than authoritarian ban-hammers.

Supervision of children

There appears to be an assumption that children roam the Internet completely unsupervised by any adult at any time, while in the offline world (to which analogies are often drawn regarding regulation of access to alcohol, pornography, or gambling) this is almost never the case.

Children are surrounded by adults who can guide and regulate their behaviour. It is only online that there is an assumption that children will be left to their own devices without any supervision or guidance. The government appears to assume that the parents of Australia are unable or unwilling to supervise their children and that it must step in and substitute itself as a parent. Rather than helping adults who want assistance, but not replacement, the government proposes heavy-handed restrictions in a misguided attempt to make the problem disappear.

It is unreasonable to expect that the responsibility for supervising children and determining what they should and should not be able to view should be shifted entirely from their parent, guardian, or other responsible adult to the government, or any private company, particularly one not based in Australia. The social mores and taboos of a foreign society should not dictate the materials that are available or not to an Australian.

Recommendation: EFA recommends that the responsibility for what material children are permitted to access should remain with their parents, guardians, and other responsible adults actively involved in their upbringing.

Changes since the Broadcasting Services Act 1992

The *Online Safety Act*[9] includes a number of important differences to the requirements for restricted access systems that were not present in the Broadcasting Services Act. The changes in scope fundamentally change the way the determination will affect access to information in Australia. A rush to legislate without due consideration of the complexity of the issue will result in harmful adverse outcomes.

The *Online Safety Act* has expanded the scope of classification to now include material that is not published in Australia, but material that is merely *accessible from* Australia. The discussion paper notes that "the RAS will only apply to Restricted Material that is provided from Australia on a social media service, relevant electronic service or designated internet service, or that is hosted in Australia."[10]

---

[9] *Online Safety Act 2021.*
[10] Office of the eSafety Commissioner, 'Restricted Access System Declaration Online Safety Act 2021 Discussion Paper' (Australian Government, August 2021) 5

Section 10 of the *Online Safety Act* defines what it means for material to be *provided on* a service:

> *For the purposes of this Act, material is provided on a social media service, relevant electronic service or designated internet service if the material is accessible to, or delivered to, one or more of the end-users using the service.*

Relevant electronic services are defined in section 13 of the *Online Services Act*:

> *(1) For the purposes of this Act, relevant electronic service means any of the following electronic services:*
>
> *(a) a service that enables end-users to communicate, by means of email, with other end-users;*
>
> *(b) an instant messaging service that enables end-users to communicate with other end-users;*
>
> *(c) an SMS service that enables end-users to communicate with other end-users;*
>
> *(d) an MMS service that enables end-users to communicate with other end-users;*
>
> *(e) a chat service that enables end-users to communicate with other end-users;*
>
> *(f) a service that enables end-users to play online games with other end-users;*
>
> *(g) an electronic service specified in the legislative rules;*
>
> *but does not include an exempt service (as defined by subsection (2)).*
>
> *(2) For the purposes of this section, a service is an exempt service if none of the material on the service is accessible to, or delivered to, one or more end-users in Australia.*

The existing restricted access system determination[11] is limited to systems that are *hosted* in Australia, not those to which access is provided from Australia. This change has increased the scope of regulated systems from Australia to the entire Internet that is accessible from Australia. This massive expansion in scope means any mistakes will have much broader impact, and thus greater care is required than was required for the original design of restricted access systems under the *Broadcasting Services Act*.

Recommendation: That the restricted access system determination explicitly takes into account the much broader scope of the *Online Safety Act* compared to the *Broadcasting Services Act*.

Regulation of private communications

Regulation under the *Broadcasting Services Act* is, as can be readily appreciated from the name of the Act, aimed at regulating communications that are *broadcast*. Communications between individuals, or among small groups, are not *broadcast* to the general public and do not require the same kinds of protections against accidental discovery that have been proposed. Regulating private communications is not a proportionate method of achieving the stated goal of "reducing the exposure of children and young people under 18 to online pornography in Australia".

<https://www.esafety.gov.au/sites/default/files/2021-08/OSA%20-%20Restricted%20Access%20System%20discussion%20paper_0.pdf>, Question 1.

[11] *Restricted Access Systems Declaration 2014*.

The *Broadcasting Services Act 1992* did not seek to regulate all private communications between individuals, and clearly limits its remit to only narrowly defined adult chat services where "it would be concluded that the majority of the content accessed by end-users of the chat service is reasonably likely to be prohibited content or potential prohibited content."

Indeed, the definition of "content service" included in the *Broadcasting Services Act*[12] explicitly excludes:

> (p) a service that enables end-users to communicate, by means of email, with other end-users;
>
> (q) an instant messaging service that:
>
> (i) enables end-users to communicate with other end-users; and
>
> (ii) is not an adult chat service;
>
> (r) an SMS service that:
>
> (i) enables end-users to communicate with other end-users; and
>
> (ii) is not an adult chat service;
>
> (s) an MMS service that:
>
> (i) enables end-users to communicate with other end-users; and
>
> (ii) is not an adult chat service;

Requiring *all* SMS, MMS, email, and chat services to implement a restricted access system would be a dramatic increase in restrictions on what forms of communication are available to Australians. This level of government intervention in private communications is disturbing in a country that claims to be a liberal democracy.

Recommendation: That any determination explicitly limits the requirement for a restricted access system to only adult content services and excludes general-purpose communications systems.

[12] *Broadcasting Services Act 1992* (n 2) Schedule 7, s 2.

Technical Feasibility

Location Requirement

The *Online Safety Act* indicates that a restricted access system needs to be enacted if material is accessible by end-users in Australia. This implies that a service will need to be able to determine the residency or physical location of an end-user in order to validate that they are in Australia.

A provider would thus need to either decide not to offer services to anyone in Australia[13], or to enact a location check for *all of their customers* in order to determine their location. This will add additional data security and privacy risk to both providers and end-users, as collection of this data will require it to be kept secure.

Recommendation: That the physical location of a customer should not be required in order to perform age verification checks.

Anonymity Requirement

The *Privacy Act 1998* requires that individuals must have the option of dealing anonymously or by pseudonym with an APP entity.[14] Assessing a person's age while also maintaining anonymity may prove impossible, and thus require an entity such as an internet service provider to violate the *Privacy Act* in order to comply with the *Online Safety Act*.

It is difficult to see how decreasing privacy promotes online safety.

Recommendation: That the identity of a customer should not be required in order to perform age verification checks.

Massive Scope

As discussed above, the scope of the proposed restricted access systems would encompass a huge range of services that are not currently subject to any requirement to classify or screen material provided using the service, and which there is no expectation to do so from customers of these services.

Adding age verification to SMS, MMS, and emails services will represent a substantial technical burden to services where age verification has never been a design consideration, while the nature of the problem to be solved has not been adequately described. This will create a substantial regulatory burden on services that do not need it.

Does person-to-person communication require an age verification check? Why? Why, then, do we not perform age verification when posting a letter or a parcel?

---

[13] VPN services can readily be used to make Internet traffic appear to originate from places other than Australia.
[14] *Privacy Act 1988* APP 2.

Recommendation: EFA recommends that all communications of a given type should be subject to the same restrictions or lack thereof.

If we are to restrict private communications between adults in a new way, a comprehensive justification of the need should be thoroughly documented to ensure that any such restriction is proportional to the need. EFA remains unconvinced that there is any such need.

Such a substantial increase in restrictions on Australians' ability to communicate privately should require the discussion and approval of Parliament after sufficient public debate to ensure that it is what Australians actually want. It should not be imposed by an unelected bureaucrat under cover of inflated claims to be protecting children from nebulous threats.

A Children's Internet?

It is difficult to see how the proposed scheme will operate without needing to create a separate, parallel *children's Internet* that only provides material suitable for the youngest children, particularly if a restricted access system requirement is imposed on entire Internet service providers.

Without such a parallel system, either adults will be unreasonably restricted from viewing perfectly lawful material, or children may be able to view material that is not specifically made for them. It is unreasonable to require adults to convert all of their communications to those suitable for consumption by 4-year-old children.

Comparisons with the offline world are often made in discussions about Internet regulation, and yet there are very few "children only" spaces in the physical world. Most of the world is accessible to both children and adults, and we rely on adult supervision to guide children towards age-appropriate materials and to educate them about what they are seeing and hearing.

We entrust adults to look after the children in their care and supervise what they do, and supervision of what children do on the Internet should be no different. We do not, for example, convert all roads to be accessible only by adults over the age of 18, despite their dangers. We allow children to catch public transport, despite what they may overhear when other adults speak to each other nearby.

We do not require age verification to send a letter to another person, so why should we require an age verification check to send a text or an email to a friend or colleague? Libraries are full of books with any number of challenging ideas, but we do not require a person to enter their age into a keypad before opening a cover and beginning to read.

The fact that a subset of children are not adequately supervised by the adults around them is a social problem, not a technology problem, and it will require social solutions, not technological ones.

There appears to be a view in some quarters that no one should ever, under any circumstances, accidentally view something that may upset them. This infantalises adults, and robs parents of the right to adjust what their children see and hear at a pace that suits their individual

development. What may be challenging for one child to see may not faze another, and it is impossible for the government to know this in advance.

Recommendation: That the government should not attempt to mandate the creation of a separate "Children's Internet".

Instead of attempting to cut children off from the real world until they are hurled—untrained, unprepared, and defenseless—into the harsh realities of the adult world at age 18, governments should focus on supporting parents, guardians, teachers, and other responsible adults to guide the children in their care so that they can grow into fully functional adults at a pace that best suits them individually.

Recommendation: That parents, guardians, and similar responsible adults should be the arbiters of what the children in their care view on the Internet.

Facial Surveillance

There have been some suggestions that facial surveillance and artificial intelligence can solve the difficult technical problems of age verification.[15]

There is now a wealth of research into the harms of facial surveillance systems.[16] The Australian Human Rights Commission has recommended a moratorium on the use of biometric technologies, including facial recognition, until the law provides stronger, clearer and more targeted human rights protections.[17] Research by the Automated Society Working Group at Monash University noted serious concerns by Australians about use of facial surveillance systems:

> *Since the use of the technology may have serious consequences for people's life circumstances, there may be a compelling case to delimit the implementation and use of facial recognition technology, as other countries and jurisdictions have done.*[18]

Given this context, advocating for the use of facial surveillance for an age verification system at this point in time could be considered at best ill-informed and, potentially, dangerously negligent.

---

[15] Jamie Tarabay, 'Australia Proposes Face Scans for Watching Online Pornography', *The New York Times* (online, 29 October 2019) <https://www.nytimes.com/2019/10/29/world/australia/pornography-facial-recognition.html>.
[16] Max Read, 'Why We Should Ban Facial Recognition Technology', *Intelligencer* (30 January 2020) <http://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html>.
[17] Australian Human Rights Commission, *Human Rights and Technology Final Report* (Commonwealth of Australia, 2021) 13 <https://nla.gov.au/nla.obj-2972857180>.
[18] Automated Society Working Group, School of Media, Film, and Journalism, *Australian Attitudes to Facial Recognition: A National Survey* (Whitepaper No 1, Monash University, May 2020) <https://www.monash.edu/___data/assets/pdf_file/0011/2211599/Facial-Recognition-Whitepaper-Monash,-ASWG.pdf>.

Learning From Failure

Other attempts at implementing age-verification systems have failed.[19] Broadband consumers in the UK overwhelmingly opt-out of optional "child friendly" filters.[20] Australians have already rejected mandatory internet filtering.[21]

The government would do well to learn from these failures and not repeat them, rather than to assume that the failure was caused by a lack of enthusiasm or vigor. Doing the wrong thing with greater gusto simply increases the destruction caused by the inevitable failure. Australian governments do not have a strong track record of learning from their own failures[22], let alone those made by others.[23] This can change as soon as governments decide they want to change.

Recommendation: EFA recommends that the eSafety Commissioner does not repeat the same mistakes that others have made attempting to implement restricted access systems.

---

[19] Timothy B Lee, 'UK Porn Blacklist Is Dead after Government Abandons Age Verification', *Ars Technica* (16 October 2019) <https://arstechnica.com/tech-policy/2019/10/uk-government-abandons-planned-porn-age-verification-scheme/>.

[20] 'New Broadband Users Shun UK Porn Filters, Ofcom Finds', *BBC News* (online, 23 July 2014) <https://www.bbc.com/news/technology-28440067>.

[21] Joel Falconer, 'Australia's Mandatory Internet Filter Has Finally Been Killed', *The Next Web* (9 November 2012) <https://thenextweb.com/au/2012/11/09/finally-australias-controversial-mandatory-isp-filtering-is-off-the-table/>.

[22] Finance and Public Administration References Committee, *Digital Delivery of Government Services, Dated June 2018.* (2018) <https://nla.gov.au/nla.obj-2829855816>.

[23] Charlie Osborne, 'UK Porn Block Collapses and I Couldn't Be Happier about It', *ZDNet* <https://www.zdnet.com/article/uk-porn-block-collapses-and-i-couldnt-be-happier-about-it/>.

Adverse Consequences

The adverse consequences from the various mechanisms proposed for creating a restricted access scheme are manifold and well documented. EFA has provided numerous examples in its many submissions to inquiries, requests for comment, panel discussions, consultations, and roundtables over the past few decades. We do not intend to re-document all of them here.

Pre-emptive Censorship

International experience indicates that platforms prefer to over-censor material rather than deal with the complexity of content moderation or classification, particularly for content they deem—often incorrectly—as sexual content.

LGBTQ+ materials are often incorrectly categorised as inherently sexual, and censored as a result.[24] By outsourcing the responsibility for censorship to private companies with a track record of prudishness and sexist content moderation[25], any restricted access system will lead to over-censorship of vulnerable and marginalised groups.

The adverse impacts of the FOSTA-SESTA legislation in the United States are well documented.[26]

All of these adverse effects were predicted in advance but were not heeded by legislators or regulators.

To guard against over-censorship, certain content categories such as sexual health and sexual education materials should be explicitly protected against removal by services subject to a restricted access system. Incorrect removal or censorship of content should result in penalties.

Recommendation: EFA recommends that certain classes of material should be explicitly exempted from restricted access systems, with penalties for incorrect censorship or removal.

Unreasonable Privacy Intrusion

Services such as SMS, MMS, email, and chat services are provided, for the most part, for private person-to-person communications that are not subject to the National Classification Code. The imposition of government-mandated classification of private communication material sent via these services represents an unreasonable intrusion into the privacy of personal communications.

---

[24] 'TikTok Apologises for Censoring LGBT+ Content', *Reuters* (online, 22 September 2020) <https://www.reuters.com/article/britain-tech-lgbt-idUSL5N2GJ459>.
[25] Emma Shapiro, 'Facebook's Censoring of Women's Bodies Is Nipocrisy', *Hyperallergic* (30 August 2021) <http://hyperallergic.com/673311/facebook-censoring-of-womens-bodies-is-nipocrisy/>.
[26] 'Erased - The Impact of FOSTA-SESTA and the Removal of Backpage 2020', *Hacking//Hustling* <https://hackinghustling.org/erased-the-impact-of-fosta-sesta-2020/>.

Undue Privacy Risks

Any age verification service will require the collection of sensitive personal information. At minimum, any such system will require:

- a person's date of birth, from which to calculate their current age
- an indication that a person is physically in Australia
- some way to authenticate that a person is the person whose age is to be verified

This information represents a valuable trove of personal data that will attract criminals seeking to monetise this personal information. Data breaches are common[27] and there are few remedies available under Australian law for breaches of privacy.[28]

These risks will be assumed by every Australian yet the benefits to them are not adequately outlined, nor is the nature of the problem sufficiently described. There may be other, privacy-enhancing or at least privacy-preserving options that provide the same benefits but these have not been explored. This approach is inconsistent with the Safety by Design[29] philosophy espoused by the eSafety Commissioner.

Recommendation: EFA recommends that alternate, privacy-enhancing solutions to content access control are explored before enacting an age-verification system.

Classification System Review

The existing classification system is under review[30], and was last updated in 2012. It does not reflect current community expectations for access to information. Failure to accommodate likely changes to the classification system will result in perverse outcomes.

Recommendation: That the restricted access system declaration incorporates any changes resulting from the review of Australian classification regulation.

Incorrect Classification

In 2009, the Australian Communications and Media Authority mis-classified a website as Refused Classification only for it to be subsequently classified as R18+ by the National Classification Board.[31] It is entirely expected that similar mistakes will be made by the eSafety

---

[27] 'Notifiable Data Breaches Report: January–June 2020', *OAIC* (26 August 2020) <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2020/> ('*Notifiable Data Breaches Report*').
[28] 'Serious Invasions of Privacy in the Digital Era (DP 80)', *ALRC* <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-dp-80/>.
[29] 'Safety by Design', *eSafety Commissioner* (2 March 2021) <https://www.esafety.gov.au/about-us/safety-by-design>.
[30] Transport Department of Infrastructure, 'Review of Australian Classification Regulation' (Text, 23 December 2019) <https://www.communications.gov.au/have-your-say/review-australian-classification-regulation>.
[31] Nicolas Suzor, Irene Graham, and Kylie Pappalardo, 'Submission to the Department of Broadband, Communications and the Digital Economy 'Mandatory Internet Service Provider (ISP) Filtering'

Commissioner, yet the *Online Safety Act* does not contain the requirement that was present in the *Broadcasting Services Act*[32] to refer classification decisions to the Classification Board. It is likely that mis-classifications will be made, and will persist, without a robust mechanism to ensure consistency between the two bodies.

Recommendation: EFA recommends that the eSafety Commissioner refer all classification decisions to the Classification Board to ensure consistency of classification decisions.

If a mis-classification occurs, the affected party should be eligible to seek a legal remedy, including compensation, for any harm experienced if the mis-classification is due to a lack of due care, diligence, and skill on the part of the eSafety Commissioner or their delegate.

Recommendation: EFA recommends that the protections from civil proceedings provided by s 221(2) and s 222 of the *Online Safety Act* should not apply if a decision is made without due care, diligence, and skill.

Compensation For Regulatory Harms

All too often governments dismiss concerns about adverse consequences that are predictable—and often predicted—in advance. This creates a perverse incentive to over-regulate (and, in some circumstances, under-regulate) and place the cost burden of their mistakes onto individuals or society at large.

EFA recommends that a compensation scheme be set up whereby individuals can seek compensation for harms incurred by mistakes made by regulators or those acting under regulator instruction.

By setting up such a fund, the government would be required to quantify the risk it is taking on behalf of others, rather than shifting all of that risk onto individual Australians as currently occurs.

If the government is unwilling, or unable, to determine the likely cost to others of its risk appetite, then it should not be permitted to take such risks. If it truly believes the risk to us is low, then it should, as the saying goes, *put its money where its mouth is*.

Recommendation: That the eSafety Commissioner set aside funds in a compensation scheme accessible by individuals and groups harmed by mistakes made by eSafety or those following eSafety's directions.

(Electronic Frontiers Australia, February 2010) <https://www.efa.org.au/main/wp-content/uploads/2010/02/2010-EFA-DBCDE-Transparency.pdf>; See also: Canberra Australian Senate, 'Senate Estimates' (Commonwealth of Australia, 23 February 2009) 102–104 <https://www.aph.gov.au/Parliamentary%20Business/Senate%20Estimates/ecactte/estimates/add0809/index>.

[32] *Broadcasting Services Act 1992* (n 2).

Detailed error expectations

It is easy, and common, for governments to claim that there is low risk of adverse effects from its decisions, or that the impact of adverse events is minimal. However, the number[33], frequency [34], and magnitude[35] of errors is often much greater than predicted.[36] The harm from these adverse events invariably falls on individuals, who often have little, if any, ability to seek a remedy.

Recommendation: That the eSafety Commissioner explicitly details the expected number and magnitude of errors per year that it deems is acceptable.

Due Skill and Diligence

EFA recommends that all entities, including government itself, be subject to a "due care, skill, and diligence" test when making decisions or using powers.

Australians expect that those entrusted with power over their lives can be trusted to act as fiduciaries with our best interests in mind. It is not unreasonable to expect that those entrusted with power over us should use this power with due care, skill, and diligence. Failure to do so should attract consequences, and those harmed by a failure to act with due care, skill, and diligence should be eligible for compensation.

EFA recommends that any protections from civil or criminal liability granted by the *Online Safety Act*, or a restricted access system determination, should only be available if an entity acts with due care, skill, and diligence. Failure to do so should enable an individual or group to seek legal remedies through the courts.

Recommendation: That any protections from civil or criminal liability are only available if an entity acts with due care, skill, and diligence.

---

[33] Paul Karp, 'Home Affairs Unlawfully Accessed Public's Stored Metadata, Ombudsman Reveals', *The Guardian* (online, 10 September 2019) <https://www.theguardian.com/australia-news/2019/sep/11/home-affairs-unlawfully-accessed-stored-metadata-ombudsman-reveals>.

[34] Chris Duckett, 'ACT Policing Had an Unauthorised Metadata Access Party 3249 More Times in 2015', *ZDNet* (29 July 2019) <https://www.zdnet.com/article/act-policing-had-an-unauthorised-metadata-access-party-3249-further-times-in-2015/>.

[35] 'Robodebt: Court Approves $1.8bn Settlement for Victims of Government's "Shameful" Failure', *the Guardian* (11 June 2021) <http://www.theguardian.com/australia-news/2021/jun/11/robodebt-court-approves-18bn-settlement-for-victims-of-governments-shameful-failure> ('*Robodebt*').

[36] Finance and Public Administration References Committee, *Digital Delivery of Government Services, Dated June 2018.* (2018) <https://nla.gov.au/nla.obj-2829855816>.