



Online Safety Bill – Reading Guide

December 2020

Benefit of Legislative Reform

The internet has brought great social, educational and economic benefits. But just as a small proportion of human interactions go wrong offline, so too are there risks online. By establishing proper protections to help keep Australians safe online, we can in turn help Australians to realise the substantial benefits that come from using the internet.

Over the past two decades, Australia has been at the forefront of online safety policy and regulation. We have had laws to deal with harmful online content since 1999 and the establishment of an eSafety Commissioner in 2015 was a world first. Australia's main legislative structures – the online content scheme contained in Schedules 5 and 7 of the *Broadcasting Services Act 1992* and the *Enhancing Online Safety Act 2015* (EOSA) – have served us well.

However, the rapid pace of technological change and the emergence of new platforms and services – including messaging apps, interactive games and live-streaming services – have given rise to new ways for users to interact online and created new risks.

That is why the Morrison Government committed to the development of a new Online Safety Act to enhance the powers of the eSafety Commissioner, boost protections for Australians, and increase the responsibility on industry to keep their users safe online.

The Government's Approach to Online Safety Reform

Like other sectors, industry must take responsibility for making sure that the digital services they develop are safe for Australians to use. This responsibility applies from the moment that new platforms, applications, or services first enter the market. Online safety features are not something to be 'retrofitted' following the launch of a new product or following commercial success. Legislation should reflect the primary responsibility of industry, and allow the regulator to assess this effort and act where industry falls short.

Sufficient powers should also be available for the regulator to quickly address known threats to online safety. An appropriately equipped regulator, with clear statutory powers, is necessary to provide industry with certainty about their compliance obligations. It is also necessary that, when Australians encounter online harms, they can be sufficiently supported.

Improving Australia's Online Safety Laws

In the lead up to the 2019 Federal Election, the Government committed to developing a new Online Safety Act to consolidate regulatory arrangements and update them in light of changes in the digital environment. In December 2019, the Minister for Communications, Cyber Safety and the Arts, the Hon Paul Fletcher MP, released a detailed proposal for reform. The Minister and the Department led a consultation process with stakeholders including non-government organisations, interested members of the public and digital businesses and service providers.

The findings of this consultation have been drawn upon to develop draft legislation, which has now been released for consultation. The Government is inviting submissions from interested individuals and organisations about how this legislation could be improved.

The consultation will remain open until 5pm (AEDT) Sunday 14 February 2021. More information, including how to participate, is available at communications.gov.au/online-safety.

Key Elements of the Bill

This document provides a thematic guide to the draft legislation, collating reference points across the Bill so readers can quickly navigate the elements most relevant to their interests. It is structured as follows:

Basic Online Safety Expectations (pg. 3)

The Bill builds upon the *basic online safety requirements* in the EOSA by establishing a framework for *Basic Online Safety Expectations* (BOSE) for providers of online services. The BOSE will provide the eSafety Commissioner with reporting powers, to hold providers accountable for meeting those expectations.

Schemes (pg. 4 – 10)

The Bill proposes five schemes to deal with different types of harmful online material. Four already exist in law (but are being appropriately updated). One is new – the adult cyber abuse scheme.

- *Cyber-bullying Scheme* – Provides for the removal of material that is harmful to Australian children. This scheme reflects the current regime in the EOSA, however reduces the take-down time for such material from 48 hours to 24 hours and extends the scheme to more services.
- *Adult Cyber-abuse Scheme* – Provides for the removal of material that seriously harms Australian adults. This scheme is new. It extends similar protections in the cyber-bullying scheme to adults, however with a higher threshold of ‘harm’ to reflect adults’ higher levels of resilience.
- *Image-based Abuse Scheme* – Provides for the removal of intimate images shared without the depicted person’s consent. This scheme reflects the current regime in the EOSA, however reduces the take-down time for such material from 48 hours to 24 hours.
- *Online Content Scheme* – Provides for the removal of harmful material in certain circumstances. This scheme reflects and simplifies the current regime in Schedules 5 and 7 of the BSA, with some clarifications of material and providers of services captured by the scheme, and extending the eSafety Commissioner’s take-down powers for some material to international services in some circumstances.
- *Abhorrent Violent Material Blocking Scheme* – Provides for the blocking of abhorrent violent material, such as images or video of terrorist attacks. This scheme is new, but mirrors existing legislation in the *Criminal Code Act 1995* (the Criminal Code).

Governance (pg. 11 – 12)

The Bill replicates the existing governance arrangements, with minor amendments to list the eSafety Commissioner as an official of Australian Communications and Media Authority (ACMA) for the purposes of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), and to clarify the eSafety Commissioner’s ability to direct staff and the Commissioner’s independence from the ACMA.

1. Basic Online Safety Expectations

Proposed provisions for the BOSE are primarily in Part 4 of the Bill. The BOSE framework is an **enhancement** of the basic online safety requirements, coupled with **new** powers for the eSafety Commissioner to require service providers to report on compliance with the BOSE.

DEFINITION	CORE BASIC ONLINE SAFETY EXPECTATIONS	REPORTING	COMPLIANCE and ENFORCEMENT	PUBLIC DISCLOSURE
<ul style="list-style-type: none"> •The Minister may determine, by legislative instrument, BOSE for a social media service, classes of relevant electronic services, or classes of designated internet services (cl45). •A BOSE determination must include the set of core principles listed in cl46 at a minimum (cl46). •In forming or varying a determination the Minister must consult with the public (cl47). 	<ul style="list-style-type: none"> •The Basic Online Safety Expectations will include, in legislation, core expectations that: <ul style="list-style-type: none"> •end-users are able to access services in a safe manner; •the extent of harmful material is minimised; •technological or other measures are in effect to prevent access by children to class 2 material; and •there are clear and readily identifiable mechanisms that enable end-users to report and make complaints about harmful material. 	<ul style="list-style-type: none"> •The Commissioner may require service providers to report on their compliance with the BOSE. Reporting may be either: <ul style="list-style-type: none"> •by a particular service provider at regular intervals (cl49); •by a class of service providers at regular intervals (cl52); •by a particular provider on an ad hoc basis (cl56); or •by a class of service providers on an ad hoc basis (cl59). 	<ul style="list-style-type: none"> •Service providers must comply with a requirement to report. This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision (clauses 50, 53, 57 and 60). •Enforcement powers are in Part 10 of the Bill. Other enforcement options are infringement notices (cl163). 	<ul style="list-style-type: none"> •The Commissioner may notify the public about a service provider's compliance with the BOSE (cl48) and BOSE reporting requirements (clauses 55 and 62). This increases transparency about providers who don't take steps to make their services safe for their end-users.

2. Cyber-bullying Scheme

Proposed provisions for the Cyber-bullying Scheme are primarily in Part 5 of the Bill. The Cyber-bullying Scheme includes minor **enhancements** on the existing scheme, and **extends** the scheme to more services.

DEFINITION	COMPLAINTS	REMOVAL NOTICES	COMPLIANCE and ENFORCEMENT	PUBLIC DISCLOSURE
<ul style="list-style-type: none"> The Bill sets out the criteria for 'cyber-bullying material targeted at an Australian child' (cl6). 	<ul style="list-style-type: none"> Under Part 3 of the Bill, a child or a 'responsible person' may make a complaint to the Commissioner about cyber-bullying material (cl30). The Commissioner may investigate such a complaint (cl31). An individual should complain to a provider in the first instance. If the relevant service provider fails to assist the individual when they raise a complaint, the individual can request that the Commissioner issue a removal notice to a provider (cl30, cl65). This reflects the expectation that industry take steps to protect their users in the first instance, and the intention for the eSafety Commissioner to serve as a safety net. 	<ul style="list-style-type: none"> The Commissioner may give a removal notice to a social media service, relevant electronic service or designated internet service (cl65), a hosting service provider (cl66), or an end-user (cl70), requiring them to take down cyber-bullying material within 24 hours. If the Commissioner prefers, and with the complainant's consent, they may instead issue a 'service provider notification' to give providers an opportunity to remove material or rectify a breach of the service's terms of use before a removal notice is needed. The Commissioner may also issue an end-user notice with requirements to apologise, or to refrain from posting cyber-bullying material targeted at the complainant in future (cl70). 	<ul style="list-style-type: none"> Service providers must comply with a removal notice. This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision (cl67). A contravention of a civil penalty provision is enforceable under Part 10 of the Bill. An infringement notice may be issued for contravention of removal notices provisions under this scheme (cl163). An end-user must also comply with a removal notice, however this is not a civil penalty provision (as in many cases the perpetrator is also child) (cl71). However, cl71 is enforceable by injunction under Part 7 of the Regulatory Powers Act (cl165). The Commissioner may choose to issue a formal warning before taking enforcement action (clauses 68 and 72). 	<ul style="list-style-type: none"> The Commissioner may notify the public about a service provider's non-compliance with a removal notice (cl69). The Commissioner may notify the public where there were two or more occasions during the previous 12 months on which cyber-bullying material targeted at an Australian child was provided on a service, and the material contravened that service's terms of use (cl73).

3. Adult Cyber-abuse Scheme

Proposed provisions for the Adult Cyber-abuse Scheme are primarily in Part 7 of the Bill. The Adult Cyber-abuse Scheme is a **new** scheme. It provides the same mechanism to have content removed as the Cyber-bullying Scheme, but with a higher threshold of harm and with the addition of civil penalties for end-users.

DEFINITION	COMPLAINTS	REMOVAL NOTICES	COMPLIANCE and ENFORCEMENT	PUBLIC DISCLOSURE
<ul style="list-style-type: none"> The Bill sets out the criteria for 'cyber-abuse material targeted at an Australian adult' (cl7). 	<ul style="list-style-type: none"> Under Part 3 of the Bill, a person or a 'responsible person' acting on that person's behalf may make a complaint to the Commissioner about cyber-abuse material (cl36). The Commissioner may investigate such a complaint (cl37). An individual should complain to a provider in the first instance. If the relevant service provider fails to assist the individual when they raise a complaint, the individual can request that the Commissioner issue a removal notice to a provider (cl36, cl88). This reflects the expectation that industry take steps to protect their users in the first instance, and the intention for the eSafety Commissioner to serve as a safety net. 	<ul style="list-style-type: none"> The Commissioner may give a removal notice to a social media service, relevant electronic service or designated internet service (cl88), a hosting service provider (cl90), or an end-user (cl89), requiring them to take down cyber-abuse material within 24 hours. If the Commissioner prefers, with the complainant's consent, they can instead issue a service provider notification, to give providers an opportunity to remove material or rectify a breach of the service's terms of use before a removal notice is needed (cl93). 	<ul style="list-style-type: none"> Service providers and end-users must comply with a removal notice. This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision (cl91). Enforcement powers are in Part 10 of the Bill. Other enforcement options are infringement notices (cl163), enforceable undertakings (cl 164) and injunctions (cl165). The Commissioner may choose to issue a formal warning before taking enforcement action (cl92). 	<ul style="list-style-type: none"> The Commissioner may notify the public where there were two or more occasions during the previous 12 months on which cyber-abuse material targeted at an Australian adult was provided on a service, and the material contravened that service's terms of use (cl93).

4. Image-based Abuse Scheme

Proposed provisions for the Image-based Abuse Scheme are primarily in Part 6 of the Bill. The Image-Based Abuse Scheme includes minor **enhancements** on the existing scheme.

DEFINITION	COMPLAINTS	REMOVAL NOTICES	COMPLIANCE and ENFORCEMENT	PUBLIC DISCLOSURE
<ul style="list-style-type: none"> •The Bill sets out the definition of 'intimate image' (cl15) and 'non-consensual intimate image of a person' (cl16). •The Bill also sets out that a person must not post an intimate image of another person without consent (cl75). 	<ul style="list-style-type: none"> •Under Part 3 of the Bill, the depicted person or an 'authorised person' acting on their behalf may make a complaint to the Commissioner about an intimate image (cl32), if it has been posted in contravention of cl75. •The Commissioner may investigate such a complaint (cl34). •The depicted person or an 'authorised person' may also give an objection notice to the Commissioner about an intimate image (cl33), even if consent was initially provided (for instance if consent is subsequently withdrawn or the person misunderstood). •The Commissioner may consider whether to give a removal notice in response to an objection (cl35). •Given the nature of the material under this scheme, a person may complain to the Commissioner directly, without a complaint being made to a provider first. 	<ul style="list-style-type: none"> •The Commissioner may give a removal notice to a social media service, relevant electronic service or designated internet service (cl77), a hosting service provider (cl79), or an end-user (cl78), requiring them to take down an intimate image within 24 hours. •If Commissioner prefers, with the complainant's consent, they may instead issue a service provider notification, to give providers an opportunity to remove material or rectify a breach of the service's terms of use before a removal notice is issued. •The Commissioner may also give a person a remedial direction, to prevent a person from contravening cl75 in the future (cl83). 	<ul style="list-style-type: none"> •Service providers and end-users must comply with a removal notice. This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision (cl80). •A person also must comply with a remedial direction. This is also a civil penalty provision, and 500 penalty units attach to a contravention of this provision. •Enforcement powers are in Part 10 of the Bill. •Other enforcement options are infringement notices (cl163), enforceable undertakings (cl164) and injunctions (cl165). •The Commissioner may choose to issue a formal warning before taking enforcement action (clauses 81 and 84). 	<ul style="list-style-type: none"> •The Commissioner may notify the public where there were two or more occasions during the previous 12 months on which an intimate image was posted on a service without the consent of the person depicted, and the material contravened that service's terms of use (cl85).

5. Online Content Scheme

Proposed provisions for the Online Content Scheme are primarily in Part 9 of the Bill. The Online Content Scheme is an **enhancement** on the existing scheme, and **extends** the eSafety Commissioner’s take-down powers for class 1 material to international services in some circumstances.

Take-down powers related to class 1 material:

DEFINITION	COMPLAINTS	REMOVAL NOTICES	COMPLIANCE and ENFORCEMENT	FEDERAL COURT ORDERS
<ul style="list-style-type: none"> •The Bill sets out the definition of 'class 1 material' (cl106). •Class 1 material includes films, publications, computer games, and all other types of material, that is classified, or likely to be classified, 'Refused Classification' (RC) under the <i>Classification (Publications, Films and Computer Games) Act 1995</i>. 	<ul style="list-style-type: none"> •Under Part 3 of the Bill, a person may make a complaint to the Commissioner if an end-user in Australia can access class 1 material (cl38). •A person may also make a complaint if they have reason to believe another person has breached a service provider rule, industry code or standard or a civil penalty provision under Part 9 (which deals with the online content scheme) (cl39). •The Commissioner may investigate such complaints (cl42). 	<ul style="list-style-type: none"> •The Commissioner may give a removal notice to a social media service, relevant electronic service or designated internet service (cl109), or a hosting service (cl110), requiring them to take down class 1 material within 24 hours. •If a website systemically ignores take down notices for class 1 material, the Commissioner may give an internet search engine service a link deletion notice to require the provider to cease providing a link (cl124). •Similarly, if an app systemically ignores take down notices for class 1 material, the Commissioner may give an app removal notice to an app distribution service provider, to cease enabling end-users in Australia to download an app (cl128). •The Commissioner may give notices for class 1 material to any of the above providers, regardless of whether the service is provided from Australia or not. 	<ul style="list-style-type: none"> • Service providers must comply with a removal notice (cl111), link deletion notice (cl125) or app removal notice (cl129). These are civil penalty provisions, and 500 penalty units attach to a contravention of them. •Enforcement powers are in Part 10 of the Bill. •Other enforcement options are infringement notices (cl163), enforceable undertakings (cl164) and injunctions (cl165). •The Commissioner may choose to issue a formal warning before taking enforcement action (clauses 112, 126 and 130). 	<ul style="list-style-type: none"> •The Commissioner may apply to the Federal Court for an order. These powers would only be applied in a worst-case scenario, where all other formal and informal attempts to remedy a situation have failed. •The Commissioner may apply to the Federal Court for an order for a: <ul style="list-style-type: none"> • social media service (cl156), • relevant electronic service (cl157), • designated internet service (cl158), or • supplier of an internet carriage service (cl159) •To stop supplying that service if: <ul style="list-style-type: none"> • the person refused to comply with a removal or remedial notice on two of more occasions in the preceding 12 months, and • as a result of those contraventions, the continued operation of that service represents a significant community safety risk. •If the Federal Court is satisfied that these conditions are met, it may order the person to cease supplying that service.

Take-down powers related to class 2 material:

DEFINITION	COMPLAINTS	REMOVAL NOTICES	COMPLIANCE and ENFORCEMENT	FEDERAL COURT ORDERS
<ul style="list-style-type: none"> The Bill sets out the definition of 'class 2 material' (cl107). Class 2 material covered by 107(1)(a), (b), (c), (d) or (e) includes: <ul style="list-style-type: none"> a film or other types of material, that is classified, or likely to be classified, 'X18+' under the <i>Classification (Publications, Films and Computer Games) Act 1995</i>, or a publication that is classified, or likely to be classified, 'Category 2 restricted' under the <i>Classification (Publications, Films and Computer Games) Act 1995</i>. Class 2 material covered by 107(1)(f), (g), (h), (i), (j), (k) or (l) includes: <ul style="list-style-type: none"> a film, 'computer game' or other types of material, that is classified, or likely to be classified, 'R18+' under the <i>Classification (Publications, Films and Computer Games) Act 1995</i>, or a publication that is classified, or likely to be classified, 'Category 1 restricted' under the <i>Classification (Publications, Films and Computer Games) Act 1995</i>. 	<ul style="list-style-type: none"> Under Part 3 of the Bill, a person may make a complaint to the Commissioner if an end-user in Australia can access: <ul style="list-style-type: none"> class 2 material covered by 107(1)(a), (b), (c), (d) or (e) (cl38); class 2 material covered by 107(1)(f), (g), (h), (i), (j), (k) or (l) that is not subject to a restricted access system (cl38). A person may also make a complaint if they have reason to believe another person has breached a civil penalty provision under Part 9 (which deals with the online content scheme) (cl39). The Commissioner may investigate such complaints (cl42) using their investigative powers as set out by Part 14 of the Bill. 	<ul style="list-style-type: none"> The Commissioner may give a removal notice to the following services provided from Australia: <ul style="list-style-type: none"> social media service, relevant electronic service or designated internet service (cl114), or hosting service (cl115), requiring them to take down class 2 material covered by 107(1)(a), (b), (c), (d) or (e) within 24 hours. The Commissioner may give a remedial notice to the following services provided from Australia: <ul style="list-style-type: none"> an Australian social media service, relevant electronic service or designated internet service (cl119), or a hosting service (cl120) requiring them to take down class 2 material covered by 107(1)(f), (g), (h), (i), (j), (k) or (l) or ensure the material is subject to a restricted access system within 24 hours. 	<ul style="list-style-type: none"> Service providers must comply with a removal notice. This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision (cl116). A person also must comply with a remedial notice. This is also a civil penalty provision, and 500 penalty units attach to a contravention of this provision (cl121). Enforcement powers are in Part 10 of the Bill. Other enforcement options are infringement notices (cl163), enforceable undertakings (cl164) and injunctions (cl165). The Commissioner may choose to issue a formal warning before taking enforcement action (clauses 117 and 122). 	<ul style="list-style-type: none"> The Commissioner may apply to the Federal Court for an order. These powers would only be applied in a worst-case scenario, where all other formal and informal attempts to remedy a situation have failed. The Commissioner may apply to the Federal Court for an order for a: <ul style="list-style-type: none"> social media service (cl156), relevant electronic service (cl157), designated internet service (cl158), or supplier of an internet carriage service (cl159). to stop supplying that service if: <ul style="list-style-type: none"> the person refused to comply with a removal or remedial notice on two of more occasions in the preceding 12 months, and as a result of those contraventions, the continued operation of that service represents a significant community safety risk. If the Federal Court is satisfied that these conditions are met, it may order the person to cease supplying that service.

Industry codes, standards, etc

DEFINITION	COMPLAINTS	DIRECTIONS	COMPLIANCE and ENFORCEMENT	FEDERAL COURT ORDERS
<ul style="list-style-type: none"> •The Bill sets out the definition of 'industry codes' (cl132) and 'industry standards' (cl133). •Matters that may be dealt with by an industry code or standard are listed under cl138. •The Commissioner may request an industry code (cl141), or may determine an industry standard (cl145). The Commissioner must consult with the public when determining an industry standard (cl148). •The Commissioner may make a service provider determination, to determine service provider rules (cl151). 	<ul style="list-style-type: none"> •Under Part 3 of the Bill, a person may make a complaint to the Commissioner if a participant of the online industry breaches an industry code (cl40). •A person may also make a complaint if another person has breached a service provider rule that applies to the second person; or civil penalty provision under Part 9 (which deals with the online content scheme) (cl39). •The Commissioner may investigate such complaints (cl42). 	<ul style="list-style-type: none"> •The Commission may give a direction to comply with an industry code to a person who has contravened, or is contravening, an industry code that applies to them (cl143). •The Commissioner may give a remedial direction to a person who has contravened or is contravening a service provider rule that applies to them, to take specified action so that the provider does not contravene the rule in the future (cl154). 	<ul style="list-style-type: none"> •Relevant persons must comply with: <ul style="list-style-type: none"> • a direction (cl143); • an industry standard (cl146); • service provider rules (cl153); • a remedial direction (cl154). •These are civil penalty provisions, and 500 penalty units attach to contraventions of these provisions. •Enforcement powers are in Part 10 of the Bill. •Other enforcement options for non compliance with a direction or an industry standard are infringement notices (cl163), enforceable undertakings (cl164) and injunctions (cl165). •The Commissioner may choose to issue a formal warning before taking enforcement action (clauses 144, 147 and 155). 	<ul style="list-style-type: none"> •The Commissioner may apply to the Federal Court for an order. These powers would only be applied in a worst-case scenario, where all other formal and informal attempts to remedy a situation have failed. •The Commissioner may apply to the Federal Court for an order for a: <ul style="list-style-type: none"> • social media service (cl156), • relevant electronic service (cl157), • designated internet service (cl158), or • supplier of an internet carriage service (cl159) •to stop supplying that service if: <ul style="list-style-type: none"> • the person contravened a civil penalty provision of this scheme on two of more occasions in the preceding 12 months, and • as a result of those contraventions, the continued operation of that service represents a significant community safety risk. •If the Federal Court is satisfied that these conditions are met, it may order the person to cease supplying that service.

6. Abhorrent Violent Material Blocking Scheme

Proposed provisions for the Abhorrent Violent Material Blocking Scheme are primarily in Part 8 of the Bill. This is a **new** scheme. This scheme introduces new powers to protect the Australian community from the same type of material captured by the *Criminal Code Act 1995*, enacted by the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*, in extreme circumstances.

DEFINITION	COMPLAINTS	BLOCKING REQUEST and BLOCKING NOTICE	COMPLIANCE and ENFORCEMENT	LIMITATIONS and EXEMPTIONS
<ul style="list-style-type: none"> •The Bill sets out the definition of 'abhorrent violent material' (AVM) (cl9). •'Abhorrent violent conduct' has the same meaning as in Subdivision H of Division 474 of the Criminal Code. 	<ul style="list-style-type: none"> •The Commissioner may receive complaints about AVM material under their general functions (cl27), but does not require a complaint to be made in order to act. •The Commissioner is required to be satisfied that availability of the material online is likely to cause significant harm, having regard to: <ul style="list-style-type: none"> •the nature of the material; •the number of end-users who are likely to access the material. •The Commissioner must also consider whether any other power conferred on the Commissioner could be used to minimise the likelihood that the availability of the material online could cause significant harm to the Australian community (cl95). 	<ul style="list-style-type: none"> •The Commissioner may give a blocking <i>request</i> to an internet service provider (ISP) to disable access to material that promotes, incites or instructs in abhorrent violent conduct or is abhorrent violent material (cl95) for up to three months (cl96). •The Commissioner may also give a blocking notice to an ISP to <i>require</i> it to disable access to material that promotes, incites or instructs in abhorrent violent conduct or is abhorrent violent material (cl99) for up to three months (cl100). •It is anticipated that, in the first instance, the Commissioner would issue a blocking request but this is not a precondition for issuing a blocking notice. 	<ul style="list-style-type: none"> • ISPs must comply with a blocking notice. There is a civil penalty provision, and 500 penalty units attached to a contravention of this provision (cl103(1)). •The Commissioner's enforcement powers are in Part 10 of the Bill. •ISPs are protected from civil proceedings when complying with a blocking notice from the Commissioner (cl221). 	<ul style="list-style-type: none"> •The Commissioner's ability to use the blocking request and blocking notice power is limited to reduce the impact on freedom of speech (clauses 95, 96, 99 and 100). •The Commissioner may not give a blocking request or blocking notice if access to the material is exempt under cl104. This clause provides exemptions for accessing AVM material in certain circumstances, such as (for example) the enforcement of laws, academic research, news reports in the public's interest, the performance of public officials, etc.

7. Governance arrangements

Proposed provisions for the governance arrangements for the Office of the eSafety Commissioner are primarily in Parts 2, 11 and 12 of the Bill. These arrangements are an **enhancement** to the existing arrangements in the EOSA.

The Bill largely replicates the existing arrangements in the EOSA. The eSafety Commissioner remains an independent statutory office holder, supported by staff from ACMA. The Bill includes small changes to clarify and enhance the eSafety Commissioner's ability to manage the Office's operations.

The Bill retains and clarifies the eSafety Commissioner's immunity from direction from ACMA (cl186), and includes a new provision to make clear that ACMA staff who support the eSafety Commissioner are subject to direction by the eSafety Commissioner. The Bill also clarifies that the eSafety Commissioner is an official of ACMA for the purposes of Commonwealth finance law (cl170). The Bill also specifically allows for the eSafety Commissioner to delegate some functions and powers to contractors (cl182).

The Bill does not include provisions from the EOSA that are no longer appropriate given the expanding role of the eSafety Commissioner. For example, it does not include expertise in 'child welfare or child wellbeing' as a criterion for appointment as the eSafety Commissioner. This is because the role has substantially expanded since it was first established as the Children's eSafety Commissioner. The Bill also does not include the ability for the eSafety Commissioner to delegate functions or powers to a body corporate.

8. eSafety Commissioner's information gathering, investigative and disclosure powers

Proposed provisions for the eSafety Commissioner's information gathering, investigative and disclosure powers are in Parts 13, 14 and 15 of the Bill respectively. These arrangements are an **enhancement** on the existing arrangements in the EOSA and the BSA.

Part 13 sets out a new power for the eSafety Commissioner to obtain information about the contact details or identity of an end-user from a social media service, relevant electronic service or designated internet service if necessary.

Part 14 of the Online Safety Bill deals with how the eSafety Commissioner conducts investigations, and replicates existing powers currently in Part 13 of the BSA. The eSafety Commissioner will have the power to summon a person by written notice to appear before the eSafety Commissioner to produce documents or to answer questions; or to provide documents or other information to the eSafety Commissioner relevant to the subject matter of the investigation.

Part 15 of the Online Safety Bill largely replicates the disclosure powers in the EOSA to enable the eSafety Commissioner to disclose information in certain circumstances, including to the Minister, APS employees for the purpose of advising the Minister, Royal Commissions, certain authorities, teachers or school principals, parents or guardians. This Part will enable the eSafety Commissioner to disclose information to a parent or guardian of an Australian child, teachers or school principals to assist in the resolution of complaints made under the Online Safety Bill, which may be particularly important in cases of cyber-bullying among school children.