Submission – Review of Online Safety Act 2021

Introduction

The purpose of this paper is to present a number of proposals that are intended to improve the safety of Online Users, including the safety of children. The proposals are focused on quickly identifying Users who might be considered bad characters. Bad characters are Users who demonstrate poor or criminal Online behaviour.

This paper is available to interested and responsible people, as well as committees and review panels who may be considering ways to address the Online safety (eSafety) issues confronting the Australian community.

A current key Online issue being discussed within the community is the impact of social media interaction on community members, particularly on children.

There is a wide array of serious issues that have become more prevalent with the widespread adoption of the Online environment by the Australian community.

The widespread adoption of Online interaction by the Australian community has increased the number of negative issues impacting community members and is increasingly being highlighted by the media and other bodies.

Most of these negative issues had already existed in the community over an extended period, but were not as widespread as they are today. The increase in Online use has increased the volume and impacts of these issues on community members, particularly on children and young adults.

There is no doubt that the Online environment has enriched the lives of most Australians by providing access to much more information and material then previously possible. But the Online environment has also become a vehicle that has enabled poor and criminal behaviour to flourish, that has destroyed and damaged lives.

The proposals in this paper are intended to improve the Online experience by reducing poor and criminal behaviour while having no, or little impact, on the millions of innocent Australian Online Users.

The benefits of the Online environment are great and for most of us it has become part of our daily lives. The Online environment cannot be “turned off”, so the negative issues that the Online environment has enabled must be addressed in a balanced way that is supported by the Australian community.

Some of the issues caused by the Online environment are serious and should be addressed quickly, but ideally with no, or minimal impact, on the lives of the majority of Australians.

Table of Contents **Page**

Objectives

The objectives of the proposals in this paper are to:

- Reduce the volume of criminal and unacceptable behaviour in the Online environment;
- Increase the speed and ease of detection of Users who have demonstrated criminal and unacceptable behaviour;
- Improve parental control over their child's Online usage;
- Leverage existing long term identity products and systems that are already in the Australian community to better support Online interaction;
- Increase community privacy by shielding private Online (legal) interactions from Australian governments, as well as Internet service providers, where the User chooses;
- Implement fast, effective, cost-efficient but seamless solutions that quickly reduce poor and criminal behaviour in the Online environment.

Online Community Problems

The negative issues confronting the Online environment are well known and most have existed before the Online environment was created. The Online environment has enabled, and in some case encouraged, poor behaviour which has become much more widespread. Below are some examples of poor and criminal behaviour that has become increasing common in Australia's Online community.

Cyberbullying

This where a person is bullied Online by one or more people. A tragic example is of 14 year-old Dolly Everett, who was bullied at school and Online. Dolly committed suicide as a result of the bullying.

Defamation

The Online environment has enabled some Users to be emblazoned to spread false claims and criticise others Online. These people are making false statements Online that they might not say directly to a person. Through the legal system some of these people have found that defamation laws apply to the Online environment such as the people who defamed the School Principal of Mt Tamborine State High School Online.

A continued widespread issue is where an Online User, who defames another, is logged on under a fake name (UserID). In this case significant effort may be required to identify the culprit.

Glorifying & Encouraging Crime

The Online environment has provided a platform for Users to "be noticed" by many others, especially on social media platforms. In a quest for notoriety some Users have engaged in criminal, dangerous and outrageous behaviour that has been posted on social media sites for the entertainment of other Users. An example was in January 2024, when four teenagers including a 15 year-old girl, stole an Audi and livestreamed the high speed Police chase that they caused, to a social media site.

Radicalisation and Terrorism

The Online environment has significantly increased access to information including unsuitable material. Some of these people are vulnerable to persuasion, such as children.

The Online environment allows a person to be accessed 24/7 including while they are in their home. This access creates a better opportunity to possibly influence the way someone thinks. This access may change a person's beliefs and may encourage a person to take an action that they may not do normally.

An example is a 16 year-old who stabbed Bishop Mar Mari Emmanuel during a church service at the Christ the Good Shepherd church in 2024. The NSW Police Commissioner labelled the attack a terrorist act.

Catfishing

Catfishing is creating a fake identity or using another person's real identity (identity theft) to engage another or others in a romantic or other type of relationship. This may be for financial gain or to upset the other person.

An example is where Lydia Abdelmalek posed Online as the celebrity Lincoln Lewis, to engage other women in a relationship. One of the victims Ms Abdelmalek engaged while posing as Mr Lewis committed suicide as consequence of the interaction. Ms Abdelmalek is currently in gaol as a consequence of this incident.

Grooming Children

The Online environment supports anonymous interaction between Users of all ages. Increasingly young children are accessing and sometimes spending long periods on social media sites and are interacting with many people, that they know nothing about.

The environment supports the ability for some people to masquerade as someone else. Routinely we hear reports where an older man has been masquerading as a young child to interact with a child for the purpose of establishing an illegal sexual relationship.

Underage Access to Information

There are very few restrictions in the Online environment to what Users can access. Users including young people, are able to access a range of unsuitable material Online such as extreme sites that display pornography, violent videos and criminal activities to name a few.

In a young person's mind, exposure to unsuitable material may become normalised. Viewing this unsuitable material may cause a change in the young person's behaviour and perception of what is acceptable in the community.

A less extreme yet still important example, is Internet sites that might change a young girl's perception of the world and herself, which might be an impact from people considered social influencers. These impacts might include a change to the young girl's perception of herself, her lifestyle and what should be important to her.

There does not seem to be one blame factor, but many young people apparently are feeling isolated. A contributing factor may be the long periods some spend Online. Concerningly the Sydney Morning Herald reports on 30 Sept 2021, that a survey showed that 50% of young girls have considered self-harming themselves. It says 18% of those girls did self-harm. It is unknown, but as stated above, possibly the high interaction with social media services may be a factor in this issue.

Excessive Time Online

The issue of excessive Online use (or screen-time) can negatively affect anyone. However it has been reported that children who suffer from too much screen time, particularly on social media sites, can have out-of-character poor behaviour such as increased mood-swings and sometimes aggressive behaviour.

Some people suffer from sleep deprivation as a result of high screen-time. Excessive screen-time might also be at the expense of healthier activities such as exercising and in-person conversations with family and friends. As a result the person may suffer long-term health issues.

Misinformation and Disinformation

Misinformation is the spreading of fake news that is not intended to influence another. Disinformation is the deliberate attempt to confuse another person or undermine confidence in an institution, such as the legal system. Social media sites provide a gateway to very large audiences that may be influenced, and therefore change their opinions, by Online disinformation sites.

Identity

A core problem with accessing Internet services is while providers may require a prospective User to register their personal details, there is little way for Internet service providers to verify the User's actual identity. Though often there is also little interest from service providers in a User's real identity.

Scope

In-Scope

The following items are addressed in this paper.

- User access to Internet services, with particular focus on social media platforms.
- Identifying Online Users who have demonstrated poor Online behaviour such as Cyberbullying.

- Identifying Online Users who have engaged in a criminal activity such as child-grooming.
- Linking of a parent to a child who uses Online services.
- Providing a parent with data on their child's Online activity.
- Supporting policy requirements that improve the safety of Users while reducing poor and criminal Online behaviour.

Out of Scope

The following items are not considered in this paper.

- General education of Users about the dangers of the Online environment.
- The education / re-education of Online Users who may be considered "at risk", such as Users who are at risk of being radicalised.
- Consideration of minimum ages for Online Users such as when a child should have the option to access social media sites.

Proposal Outcomes

The following outcomes are intended to be achieved from the proposals in this paper.

- The proposals in this paper are to be managed as a cooperation between the Federal, State and Territory governments.
- Internet service providers, particularly those who provide social media platforms, assist the Australian community in reducing the negative aspects of the Online environment.
- Poor and criminal behaviour, that occurs in the Online environment, might quickly reduce where Users are made aware that they can be easily identified. Consequently, they may quickly face the consequences of their behaviour.
- Changes to improve Online safety have no, or minimal impact on the high majority of Online Users. For instance, the preferred outcome is where the high majority of Online Users need to do nothing other than sign on to their existing Internet service provider and provide their existing identity credential – as a *once only* requirement.
- The privacy of an innocent User should continue to be protected and in fact privacy may be increased under the proposals in this paper. A User should continue to have the option for multiple UserIDs, on multiple Online platforms.

- The proposal supports Users who may be known by many names, such as nicknames, or they may use fake names. This should continue to be the case without change.

- An option that is raised later in this paper is whether parents and their young children should be linked to allow parents access to information related to their child's Online activities. This might include the child's screen-time, where they have been Online on one platform for longer than a stipulated threshold. It may be to highlight that their child has accessed restricted Internet sites, such as pornography.

Personal Identity Management

Australia does not have a national Identity card but for many years the community has used the Driver Licence as a secure, trusted, government issued personal identity document.

It is a legal requirement in most Australian jurisdictions that the Driver Licence must be with a person when they are driving, for production of the licence to Police. Consequently, the Driver Licence is one of the community's most carried identity products. It is usually kept in a person's wallet or purse.

All transport authorities issue a Learner Permit to a person who is at least 16 years of age. To obtain a Learner Permit requires the person to produce a range of identity documents to the transport authority. Once a person has been issued with a Learner Permit, they are not required to identify themselves for subsequent Driver Licence products.

The identity process and identity documents for a Learner Permit is nationally consistent.

Therefore, the identities of all vehicle drivers are known and have been confirmed by the nation's transport authorities.

The Driver Licence (including the Learner Permit) is a secure personal identity product. All transport authorities also issue interested community members with a non-driving Photo Card, that is also an identity card. Members of the community who do not drive, or no longer drive, apply for this Card as an accepted community personal identity document.

The Photo Card is known by different names across Australian states and territories but the identity process and identity documents required for a Photo Card are identical to those that are required for a Driver Licence and are also nationally consistent.

However there are inconsistencies between the state and territories in the product name, but more importantly, in the age eligibility for the Cards.

State or Territory	Card Name	Age to be eligible
NSW	Photo Card	16 yrs
VIC	Proof of Age Card	17 yrs & 11 months
QLD	Photo Identification Card	15 yrs
WA	Photo Card	16 yrs
SA	Proof of Age Card	17 yrs & 11 months
TAS	Personal Information Card	All ages
NT	Evidence of Age Card	18 yrs
ACT	Proof of Identity Card	17 yrs & 11 months

The physical securities of the Driver Licence and Photo Card that include the holder's image, are identical. Most transport authorities use facial recognition technology to reduce the risk of a person being issued with a Driver Licence or Photo Card in someone else's name.

Transport authorities hold personal details on about 90% of community members who are over 16 years of age.

The other primary personal identity document in the community is a Passport. However, many community members do not have a passport and few community members have ready access to their passport on a 24/7 basis.

Each Australian transport authority maintains an independent database of all drivers and holders of Photo Cards who have been issued with these products in their State or Territory. Many years ago transport authorities, with the assistance of the Federal Government, established the National Exchange of Vehicle and Driver Information System (NEVDIS).

NEVDIS is not a database but a gateway that connects the Driver Licence / Photo Card databases of all Australian transport authorities. It means a Policeman on the side of the road in Victoria can do an Online check of the details of a Driver Licence or Photo Card that was issued in another State or Territory.

More recently the Federal Government established the Document Verification Service (DVS). The DVS allows a range of organisations to do an Online check of a range of identity documents, including Driver Licences.

Proposals

The proposal is to require Internet service providers, particularly social media providers, to pass an Online User who seeks to register for access to their platform, to a government gateway.

The government will require the User to identify themselves using either: 1. Driver Licence or 2. a Photo Card.

The User would be required to enter details from either product, such as a Driver Licence Number and date of birth. An information match would occur in the background before the User is passed back to the Internet provider to allow the user to create a UserID and password.

However, the government would also pass back a token, such as a reference number, that the Internet provider should store with the newly created UserID.

The government would also store the same token, which may be a reference number, and an Internet service provider reference, against the User's Driver Licence or Photo Card number. Storage of these details may occur federally or within the State or Territory transport authority.

This identification process would occur *once only* at the time of UserID registration. In the future the user would log onto the Internet service provider's platform using only the UserID that they created, without any government verification process.

If a person wishes to establish a second, or additional UserID, the identification process with the government system would again occur, but again only once for the new (additional) UserID that has been created. The token or reference sent to the Internet provider would again be stored against the client's Driver Licence or Photo Card record.

The proposal means a User may have multiple UserIDs, with multiple Internet service providers. Therefore, a user with multiple UserIDs would have multiple references stored against their Driver Licence or Photo Card.

If a case of poor or criminal behaviour Online is reported to Police for investigation. The Police would request the government token, or reference, that was sent to the Internet provider, when the person registered a UserID.

The reference would reveal the Driver Licence or Photo Card number that the person used to identify themselves at the time that they created their UserID. Once the identity of the person is known, it should be possible to see reference numbers of other UserIDs that the person has created and the Internet providers that they have established accounts with. This may allow Police to easily conduct a wider investigation of the Online activities of the person.

Other enquiries may then occur with the User, given their personal and address details are readily available via the relevant transport authority.

Importantly this process continues to allow people the use of nicknames and other fake names Online. This is fine knowing that if their behaviour is not acceptable their real identities can quickly be sourced.

Privacy

The proposal is intended to maintain strong client privacy. The process of client identification occurs with government, not Internet providers. The process requires only the "most used" domestic identity documents that the high majority of adult Australians already hold.

The government will be aware that a known person is seeking access to an Internet service provider's platform but will not be aware of the UserID that the client creates. However if a complaint is made about a User a process should be established for government to be approved to ask the Internet service provider for information on the User's activities.

Whether tokens provided by government to Internet service providers, to allow a person to create a UserID and access a provider's service, are held with Federal or State / Territory transport authorities may be an important issue.

Some community members may have higher trust with the State / Territory authorities who are the issuers of the identity products used on the service. It may also reduce "Big Brother" accusations where large amounts of personal data may be held in a single Federal Government facility.

The Internet service provider should not be provided with the client's personal details.

A person may continue to choose to be known Online by multiple UserIDs including the use of fake names, which is the current situation.

Policy / Process

The proposals in this paper require a range of supporting policies. They also require supporting system development.

Internet Providers

To improve the safety aspects of the Online environment the government would require support from Internet providers including the owners of social media platforms. Legislation may be required to ensure Internet providers, 1. Pass a client to a government gateway during the User registration process, and 2. Store a government token, such as a reference, on their systems.

Later in this paper are additional Online options that the Australian community might consider beneficial for Users. If so, that would require additional system development for Internet service providers.

Online Clients

Using Driver Licence and Photo Cards for Online identity validation means the high majority of adult Online Users are already enabled to use an “identity enhanced Online environment”. However, the present State and Territory age eligibility rules, for Photo Cards, may exclude some younger people from obtaining a Photo Card. This would therefore stop their ability to access Online services.

At present there is increasing community discussion about the appropriate age for a child to access Online services. Some say that 13 years of age is too young for access to social media sites, while many people suggest 16 years is more appropriate. State and Territory transport authorities should at least consider aligning the minimum eligibility age for a Photo Card with the minimum age that the government considers appropriate to access social media sites.

It is interesting to note the Tasmanian approach to their Personal Information Card (PIC) that is available to anyone regardless of their age. Although, a young client who applies for a PIC is required to have the approval of their guardian.

In the case where a person with a PIC, who may be 10 years old, applies for a UserID to access a social media site. It is expected that the government gateway would reject the application, based on the person’s young age. In this case the gateway would not provide a token to the social media site which should stop the young client’s application for a UserID and therefore access to the site.

State & Territory Governments

Therefore under this proposal, transport authorities should align the eligible age to obtain a Photo Card with the minimum age that children are allowed to access social media sites.

However, there should be no impact if transport authorities, such as Tasmania, allow children under the approved social media access age to obtain a Photo Card. The government gateway should stop an underaged child from registering a UserID and accessing to a social media site.

Federal Government

A key task for the Federal Government is to lead the effort to improve the Online environment and engage with community leaders. If the community agree that change is required, it is assumed that legislation will be required that is best managed at a national level.

The development of a national Online government gateway would also best be coordinated federally though whether the validation gateway occurs through the National Document Validation service or the NEVDIS or another service would be determined in due course.

Options

The validation of a person's identity including their age, allows the community to consider a number of child, and other related, options to increase Online safety. In these cases, the government gateway would provide this enhanced advice to an Internet service provider. Noting the below and other features may require increased development by Internet service providers.

Guardians

Community members may see value in requiring the approval of a child's guardian for a child to access certain sites, such as social media sites. In this case, both the child and their guardian would input their identity details into the government gateway. The entry of the guardian's details would be deemed approval for the child to access the particular social media site. This should be a *once only* process for the guardian, unless the child seeks access to other social media sites.

Screen-Time / Restricted Sites

The community may wish guardians to be notified (by email or SMS) when their child has spent excessive time on an Internet site, such as a social media site. Similarly, a guardian may wish to know if their young child has accessed restricted sites, such pornography or terrorist recruitment sites.

Access Times

Some guardians may wish that their children are restricted from some sites at particular times. For instance, a guardian may not want their child to be interacting on social media between the hours of midnight and 6am.

Age Differences

The community may wish children to be better protected from Online predators who may intend to "groom" a child. For instance, it may be that a child interacting Online with another User, sees an indicator that the other person is under 18 years old. The absence of the "under 18 year-old indicator", means a child is alerted that the person they are speaking to Online may be much older than them.

Restrict Access

The government gateway validates a person’s identity document before providing a token (approval) to the Internet service provider. The service provider then allows a UserID to be created.

In the case where a client may be restricted by court from using Internet services, the government gateway might support the court order by not providing a token to an Internet service provider. Therefore no UserID can be created.

Note that following the proposals in this paper ensures that the government already knows the accounts a person has with various Internet service providers, as a result of Police enquiries. Accordingly, Government may notify service providers to suspend the User’s account.

Resistance

It is expected that the Community will strongly support attempts to improve the safety of Online Users. However, in the past the Australian community has resisted efforts by the Federal Government to better manage personal identity through proposals to issue national identity cards. The Driver Licence and Photo Card products have been adopted by the community instead of a national identity product.

The government should not underestimate community concern about tampering with personal identity. The stealing of large amounts of data on Australians from central databases, such as Optus and Medibank, by hackers, have put the community on edge about the security of their personal data. Using identity to improve Online safety must be managed carefully and be well communicated to the community.

Any change to the current Online environment will require system development that may be resisted by Internet service providers. Some service providers might only agree to changes when faced with legislation that includes significant penalties for non-compliance.

The changes proposed will have minimal impact on most Internet Users. The high majority of adult Australians already have a Driver Licence or Photo Card that they would need to use, before creating a UserID. However, there may be a small lead-time for young children to obtain a Photo Card.

Transport authorities may need to align the eligibility age for a Photo Card with the approved age for access to social media and other Internet sites.

System development may be required to establish a government gateway, though enhancement of the National Document Verification Service or the NEVDIS service are two existing options. System enhancement would also be required to store tokens or references issued to Internet service providers that relate to Driver Licence and Photo Card holders.

Conclusion

The high adoption of Internet services by Australians has changed the landscape and the futures of many Australians. However, for a minority of Internet Users they have been damaged by the negative aspects of Online interactions.

The Online issues this minority are facing today, are serious and need to be addressed quickly. If government takes no corrective action, then the negative issues will continue with more and more Australians, particularly the young, being damaged. Potentially seriously damaging future generations of Australians.

The proposals contain in this paper revolve around a *once-only* government managed identity process. Knowing the real identity of a User allows government the opportunity to quickly correct a person's poor Online behaviour. It may also discourage Online criminal behaviour where the criminal knows it is likely that he will face the consequences of his behaviour.

This can be done while maintaining a high level of privacy for Internet Users. The government will not be aware of a person's UserID/s. An Internet provider will not be aware of a person's real name unless the person chooses to provide it. This proposal supports the continued Online use of fake names, by some people.

The process uses an identity credential that is already held by the high majority of adult Australians. While there is some system development and legislation required, implementation of such a service may be quite fast given there would *not be a need to rollout a new identity credential* to the Australian community.

Using the most trusted domestic identity product is also more likely to be supported by the community in general, particularly as most community members who are Online are not required to do anything. With the roll-out of these proposals, and appropriate communication to the community, Online behaviour is expected to quickly improve.

The success of changes to improve eSafety are unlikely without the strong approval of the community, Federal, State and Territory governments and strong legislation that supports the proposals. Obviously that legislation should ensure the long-term cooperation of existing and future Internet service providers.

Please contact me for further information.

Submission written by: Steve Venning.
[redacted]

End