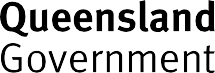




**Social media and identity verification** Queensland Department of the Premier and Cabinet research paper

September 2020

# Executive Summary

This paper presents a review of the literature pertaining to recommendation 21 of the Queensland Anti-Cyberbullying Taskforce Report, which reads:

*“The Taskforce recommends the Queensland Government, individually and/or in collaboration with the Commonwealth Government and other state and territory governments, undertake or commission research into the efficacy of requiring social media companies to implement identity verification.”*

Several countries have started to develop regulations requiring age verification in order to access online pornography or engage in online wagering. While age verification is not identity verification, similar problems could be experienced in efforts to introduce either. However, it is important to note that age verification is markedly different to identity verification. Age verification has benefits in helping to stop children from stumbling across or accessing pornography online, or from engaging in online wagering, but will only have a limited impact upon cyberbullying. This is because it does not address the underlying issues often used to perpetrate cyberbullying – the creation of fake accounts.

Some countries around the world, such as India and Brazil, have started to consider legislation aimed at requiring identity verification by social media. China already has very strict controls over all media, including social media, which encompass identity verification requirements. A real name verification system was implemented, and eventually ruled unconstitutional, in South Korea between 2007 and 2012. Few of the social media companies appear to have initiated any identify verification policies: Facebook has recently announced that viral posts from unverified accounts will have limited reach; and Twitter has a (currently suspended) verification system that Twitter users of public interest could previously apply for by submitting identity documents.

Several options exist for online identity verification, such as through a third-party provider, a government agency, or by the social media provider itself.

From the material examined, it is considered both technologically and procedurally possible for social media companies to implement identity verification. As the regulation of the internet is generally a Federal Government responsibility under the Constitution of Australia, it is considered that ultimately a national focus would be needed to ensure that telecommunication firms deny service to any companies not complying with regulations.

The findings of this paper in relation to identity verification are in alignment with the House of Representatives Standing Committee on Social Policy and Legal Affairs report tabled in March 2020 titled *Protecting the age of innocence: Report of the inquiry into age verification for online wagering and online pornography* in relation to age verification.

This paper concludes that a national focus would be needed to advance the issue of identity verification. The Queensland Government could advocate for the Federal Government to direct and adequately resource the eSafety Commissioner to develop a roadmap to examine the implementation of mandatory online identity verification for social media. It is also considered that the eSafety Commissioner could consult with the Federal Government Digital Transformation Agency in relation to the development of appropriate technical standards for identity verification and an identity verification exchange.

# Introduction

## Queensland’s Anti-Cyberbullying Taskforce

In February 2018, the Honourable Annastacia Palaszczuk MP, Premier and Minister for Trade, established the Queensland Anti-Cyberbullying Taskforce (the Taskforce) to develop a framework to address cyberbullying of children and young people in Queensland, and recommend community and government action. The Taskforce was made up of a range of independent experts.

In progressing its work, the Taskforce undertook extensive community consultation, including holding 59 consultation sessions across the State and receiving 364 written submissions. The Taskforce heard from a range of stakeholders, including children and young people who had themselves experienced cyberbullying.

The Taskforce’s report titled *Adjust our Settings: A community approach to address cyberbullying among children and young people in Queensland* was delivered to the Queensland Government in September 2018. The Taskforce recommended action by governments, parents, carers, children and young people, schools, social media companies, sporting and community organisations, universities and training providers to help reduce cyberbullying.

The Queensland Government accepted all 29 recommendations made by the Taskforce. In the Queensland Government Response to *Adjust our Settings,* the Government committed to urgently seek to engage with social media companies and encourage them to partner with governments to provide safer online platforms for children and young people. The Premier’s Foreword called on social media companies to be partners with government in taking a leadership role in protecting the safety and wellbeing of children and young people online.

### Taskforce findings and recommendations

The Taskforce found that despite the many benefits of social media, participation in social media has put children and young people at risk of cyberbullying. In its Report, the Taskforce noted that “Recent studies indicate up to 25 per cent of children and young people had experienced cyberbullying in the previous 12 months”[[1]](#footnote-1) and that “Social media is the most common platform for cyberbullying”.[[2]](#footnote-2)

The Taskforce defined social media as including “websites, computer programs, and apps that allow people to communicate and share content, including user-generated content, through messaging services and platforms such as Facebook, Instagram, Twitter, Snapchat, Google+ and YouTube”.[[3]](#footnote-3)

The Taskforce in the report *Adjust our Settings* defined cyberbullying as “an ongoing misuse of power in relationships through usually repeated verbal, physical and/or social behaviour that is intended to cause physical and/or psychological harm”[[4]](#footnote-4), and notes that bullying can happen in person or using digital or other technologies.

The Taskforce recommended social media organisations boost their efforts to manage harmful online behaviour and ensure age-appropriate use of their platforms. In response to the submissions and consultations calling for social media companies to take greater responsibility in preventing cyberbullying, the Taskforce made five recommendations regarding social media companies:

**Recommendation 21**: The Taskforce recommends the Queensland Government, individually and/or in collaboration with the Commonwealth Government and other state and territory governments, undertake or commission research into the efficacy of requiring social media companies to implement identity verification.

**Recommendation 22**: The Taskforce recommends the Queensland Government, individually and/or in collaboration with the Commonwealth Government and state and territory governments, require social media platform providers to:

* make the maximum privacy settings the default settings for all users
* make a link to privacy settings clearer, up front and more user accessible, including regular promotion of privacy settings to users
* make blocking more readily viewable and available
* implement 'safety by design' principles
* make their educational and safety materials easy to find, and regularly promote those materials to users.

**Recommendation 23**: The Taskforce recommends the Queensland Government, through Advance Queensland or other sources and in collaboration with social media companies, universities and business, examine opportunities to support the development of applications and machine-learning algorithms to detect cyberbullying.

**Recommendation 24**: The Taskforce recommends the Queensland Government, individually and/or in collaboration with the Commonwealth Government and state and territory governments, take steps to ensure social media companies:

* improve the visibility, consistency and accessibility of reporting tools on their platforms
* include a link directly to the eSafety Commissioner for users who are not satisfied with action taken by the social media company
* include messages on their platforms to remind users of the harm cyberbullying can cause and steps on how to report.

**Recommendation 25**: The Taskforce recommends the Queensland Government call on the Commonwealth Government to amend the *Enhancing Online Safety Act 2015* to provide the eSafety Commissioner with powers to require annual publication of detailed data on complaints and response times by social media platforms.

All five of these recommendations were accepted by the Queensland Government.

**The efficacy of requiring social media companies to implement identity verification -recommendation 21**

In making its recommendation 21 to the Queensland Government, the Taskforce explored the role of social media in reducing cyberbullying. The Taskforce echoed the concerns of stakeholders and the community in suggesting that social media companies and platforms needed to ensure a level of responsibility for the safety and wellbeing of their users.

During its consultation, stakeholders told the Taskforce there should be age-appropriate access to social media and requirements to prevent underage access in order to reduce the number of young children using social media. Stakeholders also commented on the need to verify social media accounts before they could be opened, as way of preventing anonymous users and fake accounts that could cyberbully children and young people.

In its report, the Taskforce carefully considered the benefits and risks of recommending verification of user identity before a social media account is opened. The Taskforce considered the impact verification of identity would have on children and young people, and the risks to their privacy, including risks of hacking, location disclosure, social profiling, third-party personal information disclosure and public and private organisations’ use of social network websites.

The Taskforce concluded the efficacy of requiring social media companies to implement verification of the identity of proposed account holders should be further explored, by the Queensland Government in collaboration with the Federal Government and State and Territory Governments. The Taskforce noted its view that this work should include consideration of privacy.

This paper therefore focuses on recommendation 21 with the remaining recommendations of the report being delivered through a range of other activities and mechanisms.

# Methodology

This paper presents a review of the literature pertaining to recommendation 21, that is, the efficacy of requiring social media companies to implement identity verification. This paper limits itself to that recommendation 21 issue and does not explore any of the other recommendations which are being addressed via other mechanisms.

The information contained in this paper is based upon a broad jurisdictional and international scan conducted by the Queensland Government Research and Information Library of any literature relating to requiring social media companies to implement identity verification.

It should be noted that although academic scholarship is included in this paper, none of the information uncovered by the literature scan specifically pertaining to the efficacy of requiring social media companies to implement identity verification could be considered academic research. Apart from submissions to and the reports from of a small number of government enquiries, the literature consisted mainly of commentary by experts, social commentators or journalists from around the world. Very little of this commentary has originated from Australia. The amount of information published on this issue is limited.

# Acknowledgements

This paper has been reviewed by the Queensland Government’s independent Anti-Cyberbullying Advisory Committee.

The paper has also been subject to an academic peer review by Dr Emily van der Nagel, Lecturer in Social Media, Communications and Media Studies, School of Media, Film and Journalism, Monash University.

# Social media

In undertaking its work, the Taskforce defined social media as “Websites and applications that enable users to create and share content or interact with others.” The Taskforce report further clarified that:

“Social media includes websites, computer programs, and apps that allow people to communicate and share content, including user-generated content, through messaging services and platforms such as Facebook, Instagram, Twitter, Snapchat, Google+ and YouTube. User-generated content has given people unprecedented access to other people’s content, which can be used positively or negatively.”

Social media is a rapidly growing field with many hundreds of social media companies clamouring for users. US digital publisher Search Engine Journal rates the top seven social media companies as Facebook (founded 2004, 2.45 billion active monthly users), Twitter (founded 2006, 330 million active monthly users), LinkedIn (founded 2003, 310 million active monthly users), Instagram (founded 2010, 1 billion active monthly users), Snapchat (founded 2011, 360 million active monthly users), Pinterest (founded 2010, 322 million active monthly users), and Reddit (founded 2005, 430 million active monthly users).[[5]](#footnote-5) While YouTube does not appear in this list, it is reported to have 2 billion actively monthly users[[6]](#footnote-6) and, as can be seen below, is very popular with young people. All of these social media companies have their headquarters in the United States. TikTok is a newer social media platform only established two years ago but has more than 800 million monthly users and is headquartered in China.[[7]](#footnote-7)

In Australia in 2020, 71 per cent of the Australian population, or 18 million Australians, actively use social media. Of all internet use, 1 in 3 minutes online is spent on social media.[[8]](#footnote-8) Research by Roy Morgan indicates that while Facebook continues to be Australia's most-used social media platform, YouTube and Instagram are more popular than Facebook for those born after 1990. TikTok is especially popular with young Australians, with more than two-thirds of the 1.6 million Australian TikTok users aged under 25.[[9]](#footnote-9)

A survey of 150 teenagers (aged 14 to 17 years) in 2017 by the Australian Psychological Society[[10]](#footnote-10) reported that the social media platforms they most commonly used were Facebook (80.8 per cent) and YouTube (72.4 per cent). Instagram was used by 66 per cent of teenagers, Snapchat by 64.7 per cent, and Twitter by 27.6 per cent. This survey reported that young people use social media for an average of 3.3 hours each day, on five or more days of the week, and some teens log onto their favoured channels as many as 50 times per day.

A random sample of more than 3000 young people in Australia aged 8 to 17 years in the 12 months to June 2017 (Kids – 8 to 12 years and Teens – 13 to 17 years) undertaken by the Office of the eSafety Commissioner[[11]](#footnote-11) found that the top five social media services used were:

* YouTube – Kids 80 per cent, Teens 86 per cent
* Facebook – Kids 26 per cent, Teens 75 per cent
* Snapchat – Kids 26 per cent, Teens 67 per cent
* Instagram – Kids 24 per cent, Teens 70 per cent
* Google+ – Kids 23 per cent, Teens 29 per cent.

During the Taskforce’s consultation, many submitters and stakeholders commented on the amount of time children and young people spent on social media platforms. A variety of benefits for children and young people from using social media have been identified including:[[12]](#footnote-12)

* **Having fun, sharing interests, and exploring identities.**
* **Making and maintaining friendships:** social media helps to maintain relationships with family members who live far away, as well as staying in touch with friends.
* **Connection and belonging:** children can connect with online global communities which share similar interests, such as games, TV series, music or hobbies as a well as a large range of issues that may be of concern to our youth. Social media removes distance boundaries and allows the forming of bonds beyond borders. For children with a disability who may have troubles in communicating and connecting with others, social media can be a great way to enable them to share their ideas and interests.
* **Digital media literacy:** online communication is now part of everyday life so exploring and experimenting on social media can help children build knowledge and skills to enjoy online activities and avoid online risks, as well as enabling them to interact more often with family and friends. Developing a positive digital footprint prepares them for future workplace opportunities allowing them to share their achievements and showcase their talents to attract the attention future employers.
* **Collaborative learning:** children can learn about and appreciate different perspectives and worldviews, and they can gather information about issues which interest or impact themselves or their friends. Through the sharing of educational content, children can both discover areas of interest and use information in formal school settings.
* **Creativity:** children can be creative with their profile pages, memes, photos, video uploads, and by developing modifications for games. Kids can share their talents whether it be writing, singing, acting, demonstrating a particular skill or ability, or just expressing themselves online. Social media also increases the opportunities to campaign for social good. Social media can help young people support or raise awareness of an important cause and make an impact in their community. It also exposes kids to important issues from around the world and allows them a voice in those issues.
* **Mental health and wellbeing:** social media can help to reduce feelings of isolation, not only by providing more avenues to make and maintain friendships, but also by helping kids develop social skills which are useful in face-to-face world communications. Young people can find support when feeling marginalised or alone, or alternatively offer support to friends and family who may be experiencing problems on a particular issue. Without having to leave their homes, kids can tap into support networks for a huge variety of issues such as medical conditions, disabilities, teenagers who are same-sex attracted, and issues such as drug addiction and eating disorders.

While significant negative consequences of social media use alone have not been conclusive in published studies, some research has found excessive use can be problematic for children and young people, including putting their education, work and relationships in jeopardy.[[13]](#footnote-13) Risks of social media use include:[[14]](#footnote-14)

* Exposure to inappropriate or upsetting content such as mean, aggressive, violent or sexual comments or images, and including deliberately accessing inappropriate content such as pornography
* Young people uploading inappropriate content like embarrassing or provocative photos or videos of themselves or others. Teenagers are often not thinking about immediate effects of these uploads, let alone the possible impact on future employability
* Inadvertently or being tricked into sharing personal information with strangers, for example, phone numbers, date of birth or location
* Emotional wellbeing impacts such as developing ‘addictions’ where young people spend too much time and effort engaging in social media. Young people may also place too much importance on features of the applications (such as obtaining ‘likes’ or other good reviews or ratings) or their self-esteem may be affected if they do not realise that social media feeds are to some extent manufactured reality often showing only the positive highlights of people’s lives such as holidays, achievements, parties, etc.
* Cyberbullying
* Exposure to unwanted or an overabundance of targeted advertising and marketing
* Unwanted sharing of personal information or images, either accidentally by friends or family, deliberately to cause embarrassment, or through data breaches, such as being hacked or having personal data sold on to other organisations.

The focus of this paper is cyberbullying, and while identity verification is likely to reduce the amount of cyberbullying experienced though social media, it is unlikely to address many of the other risks.

The Office of the eSafety Commissioner’s submission to the Taskforce said the key forms of cyberbullying behaviour from complaints received in Queensland and around Australia include:

* Nasty comments, serious name calling and incitement to suicide
* Impersonation, fake and hate pages
* Offensive or upsetting posts, sextortion or private pictures and videos shared
* Unwanted contact and threats of violence.

An Australian study has found that children and young people subject to cyberbullying report significantly more social difficulties, higher anxiety levels and depression than those subject to traditional bullying.[[15]](#footnote-15) The Australian Psychological Society submission to the Taskforce also stated:

“The serious psychosocial consequences of cyberbullying include fearing for one’s safety, impaired social and emotional adjustment; poor academic achievement, anxiety, depression and suicidality; poorer physical health; higher absenteeism; and increased loneliness and low self-esteem, and in some cases suicidal ideation”.

Use of social media can lead to behaviours which lack empathy and compassion in children. Participation in social media has put children and young people at risk of cyberbullying, which may have profound psychosocial outcomes including depression, anxiety and severe isolation.[[16]](#footnote-16)

The Taskforce report states that “Social media is the most common platform for cyberbullying.” In submissions and consultations people almost unanimously agreed social media companies should take greater responsibility for preventing or reducing cyberbullying.

No Australian social media companies were found during the course of preparing this paper and if any exist, their user base would be quite small. All of the most popular social media companies are headquartered overseas. This situation limits the levers that Australian governments have available to them to influence the behaviour of social media companies.

More discussion of the Australian context relevant to internet legislation is presented later in this paper. In addition, Australia has quite a small population in comparison with many other counties in the world. The influence Australian governments or users have with companies whose user bases are measured in the hundreds of millions or even billions is therefore quite limited.

# Identity verification

## What is identity verification?

In a traditional in-person interaction, an individual presents themselves to a company, institution or organisation (store, bank branch, commercial office, tax agency, employment service, etc.) and delivers one or more identity documents (driver’s licence, passport, etc.). At the same time, an agent can verify that the photograph and information on at least one of these identity documents corresponds with the person who is delivering the documents.

**Online identity verification** has the same goal of ensuring a person’s identity matches the one that it claims to be. It can be accomplished in a variety of ways, some more reliable and secure than others. One method to verify the identity of people remotely or online is through the use of images, in addition to electronic copies of the relevant identity documents. Another more secure method is via streaming-video identity verification using the camera and microphone from a device such as a computer, tablet, or mobile phone.

Some businesses use an identity verification service or application to assist in authenticating a person’s identify and personal information. For example, Australia Post conducts more than 8 million identity checks annually through its Digital iD program.[[17]](#footnote-17)

Services include:

* **Identity Document Verification:** checking a customer’s identity documents back to trusted issuer records.
* **Know Your Customer checks:** accessing a wide range of industry and proprietary data sources, to help businesses meet their anti-money laundering compliance obligations and identify politically exposed persons, sanctioned, and other high-risk individuals.
* **Biometric Verification:** face matching technology to help reduce the risk of identity fraud.
* **Police Checks and Workforce Verification**: providing businesses with secure, fast and convenient screening of employees and candidates.
* **Digital Cards:** an app to allow businesses to issue digital versions of their cards, licences and accreditations directly to their users and customers.

Everyday Australians also use Digital iD so they can quickly and easily share their pre-verified identity information with organisations rather than going through the full application process. Digital iD’s smartphone app is accepted as proof of age to enter participating licensed venues and to purchase alcohol in Victoria, Tasmania, Queensland, South Australia, the Australian Capital Territory and the Northern Territory (excluding takeaway alcohol in the Northern Territory).[[18]](#footnote-18)

## The current situation

Currently, there is no verification associated with the *creation* of any social media account, only a retroactive verification process on platforms like Twitter. The creation of an account on most social media platforms may involve an age check as described below, but this is easily fabricated. Verification on social media usually involves users submitting identity documents through a form on the platform, and having their identity affirmed.

### Age checking

The minimum age to open an account on most social media applications such as Facebook, Twitter, Instagram, Pinterest, Tumblr, Kik and Snapchat is 13 years old.[[19]](#footnote-19) YouTube requires account holders to be 18, but someone 13 years or older can sign up with parental permission. This age restriction exists because the majority of social media services are domiciled in the United States where companies are bound by the federal Children’s Online Privacy Protection Act (COPPA),[[20]](#footnote-20) which currently stipulates that services cannot collect personal information about users who are under the age of 13.

Most social media platforms have some sort of age checking (as opposed to age or identity verification) such as the requirement to enter a date of birth when creating an account. However, it is widely acknowledged that the simple fabrication of a date of birth is an easy work around to this requirement. The Taskforce’s consultations confirmed many young people under 13 years of age commonly hold social media accounts, as a date of birth can be easily fabricated.

### Age verification

Several countries have started to develop regulations requiring age verification in order to access online pornography or engage in online wagering. While age verification is not identity verification (as it verifies just one element of identity), a discussion on implementing age verification is warranted given similar problems could be experienced in efforts to introduce either. Similar to the description for online identity verification in the previous section of this paper, using the camera and microphone from a device it is often quite simple to ascertain that a person is over 18 and thus age verified in order to access online pornography or engage in online wagering. Using such a technique means that age verification can be accomplished without knowing the person’s identity or even their date of birth.

Work on regulating age verification includes developments in the United Kingdom. On 27 April 2017, the *Digital Economy Act 2017*[[21]](#footnote-21) was enacted requiring all online commercial pornography services, accessible from the United Kingdom, to include age verification provisions to prevent children from accessing inappropriate content. The British Board of Film Classification developed a set of criteria to assess whether the requirements of the *Digital Economy Act 2017* had been met by the age verification products of the service provider, including information about compliance with data protection legislation.

However, in late 2019 in the United Kingdom, after years of technical troubles and concerns from privacy campaigners, the plans to introduce the nationwide age verification system for online pornography have been abandoned by the government. “Despite repeated reassurances from pornography websites and age verification sites that personal details would be kept separate from information about what users had watched, privacy campaigners continued to raise concerns about data security”.[[22]](#footnote-22) It was also reported that a number of British businesses that had invested heavily in developing verification products in the hope of capitalising on large numbers of Britons wanting to verify their age in order to view legal pornography, with one age verification provider expecting a potential market of up to 25 million people.

In June 2020, France’s Parliament unanimously agreed to introduce a nationwide age verification system for pornography websites with the choice of age verification mechanisms left up to the service providers. One of the most troubling legislative tasks for any regulator has been finding a way to enforce local laws on foreign services.

In an attempt to address this problem, the French audiovisual regulator (the Conseil supérieur de l'audiovisuel, abbreviated CSA) will be granted new powers. After a first warning from the CSA, if a site does not comply with identity verification requirements within 15 days, the regulator will be able to apply for a court order to instruct telecom operators to block the access to this non-compliant site from France. A final vote in France’s Senate is still necessary for this legislation to be enacted. It is also reported that Italy approved a similar bill in late June 2020.[[23]](#footnote-23) However, critics have stated that “it is very simple to use a virtual private network (VPN), so that one's computer simulates a connection from a location outside of France, thus bypassing national legislation”.[[24]](#footnote-24)

No legislation requiring age verification for online pornography or wagering has been enacted in Australia. However, the House of Representatives Standing Committee on Social Policy and Legal Affairs recently held an inquiry on the issue and tabled a report in March 2020 titled *Protecting the age of innocence: Report of the inquiry into age verification for online wagering and online pornography.*

This inquiry considered the potential role for age verification technology in protecting children and young people in Australia from exposure to online wagering and online pornography. The report supported the implementation of online age verification in Australia and stated that “the technology for online age verification has become more sophisticated, and there are now a range of age-verification services available which seek to balance effectiveness and ease-of-use with privacy, safety, and security”.[[25]](#footnote-25)

Other recommendations from this report might also be useful in the consideration of identity verification for social media and will be discussed later in this paper.

However, it is important to note that age verification is markedly different to identity verification. Age verification has benefits in helping to stop children from stumbling across or accessing pornography online, or from engaging in online wagering, but it will only have a limited impact upon cyberbullying because it does not address the issue of fake accounts which are often used to perpetrate cyberbullying.

## Would identity verification help reduce cyberbullying?

The Taskforce noted that:

“The explosion in use of social media can lead to behaviours which lack empathy and compassion in children. Participation in social media has put children and young people at risk of cyberbullying, which may have profound psychosocial outcomes including depression, anxiety and severe isolation”.[[26]](#footnote-26)

The Taskforce further noted that “Stakeholders expressed a lack of trust in social media providers to respond adequately to complaints of online harassment or bullying”.[[27]](#footnote-27)

It has been widely reported that when people make up profiles and do not have to prove their true identity they can more readily engage in bullying and abusive behaviour[[28]](#footnote-28). Commentators from around the world are calling for more protections from these fake social media accounts:

“With a single, digital identity and verified details, the misuse of online platforms can be quashed. Individuals can quickly, simply and securely prove their age or identity online. This protects underage users from creating accounts and being targeted by adults with malicious intent, and individuals are also reassured of the identity of the people they meet online”.[[29]](#footnote-29)

However, other research has found that people still engage in bullying, harassment, and abuse on social media when they have signed up using their full names. Researchers Leonie Rösner and Nicole Krämer conducted a laboratory experiment that found that aggressive social norms led to more aggressive language, where anonymity had no direct effect.[[30]](#footnote-30) In an Australian context, while some racist abuse comes from anonymous or bot accounts, plenty comes from named people, like a racist cartoon by Bill Leak published in The Australian and widely circulated on Twitter.[[31]](#footnote-31)

A variety of authors have tried to estimate how many fake social media accounts exist. In a recent study by the NATO Strategic Command Centre of Excellence,[[32]](#footnote-32) researchers hired 16 ‘manipulation service providers’, a growth industry feeding the demand for phony clicks and likes, most based in Russia, to buy fake online engagement for 105 posts on Facebook, Twitter, YouTube and Instagram. They spent just 300 euros (a little less than 500 Australian dollars) which bought them 3530 comments, 25,750 likes, 20,000 views and 5100 followers. By studying the accounts that delivered the purchased interactions, the researchers were able to identify 18,739 inauthentic accounts that were used for social media manipulation purposes. Other researchers have estimated that 16 per cent of all Facebook accounts are fakes (5 per cent or about 137 million accounts) or duplicates (11 per cent or about 275 million accounts).[[33]](#footnote-33)

Facebook’s own latest Transparency Report reveals it ‘disabled’ 6.5 billion fake accounts, defined as “accounts created with malicious intent to violate our policies and personal profiles created to represent a business, organization or non-human entity, such as a pet”,[[34]](#footnote-34) between January and December 2019. This represents a 97 per cent increase over the 3.3 billion fake accounts it removed in 2018. In the first quarter (January-March) of 2020 it removed another 1.7 billion. Clearly, the fact that 1.7 billion fake accounts can exist so soon after 6.5 billion are removed indicates that fake accounts are continually being created. No research could be uncovered which estimates what proportion of these fake accounts are used to engage in cyberbullying or what proportion of cyberbullying originates from fake accounts.

As stated by another commentator over two years ago:

“Some form of identity verification in social media would guarantee that every account is linked to a registered user. Call it a license or a permit or whatever. But each user must register with a real name, a real address, be issued an account number and perhaps a secret code. Not unlike the security surrounding credit cards today. Without it, you can’t open a Facebook or Twitter or Instagram or YouTube account”.[[35]](#footnote-35)

It is important to note, however, that having more than one account on the same social media platform is not always indicative of trolling, harassment, or cyberbullying.

## Why would someone want to be anonymous on social media?

Much academic scholarship on social media identities claims the self is fragmented, multifaceted, and contextual.[[36]](#footnote-36) People have long created anonymous or pseudonymous social media accounts for a variety of non-harmful purposes, from avoiding discrimination to embracing creativity and play[[37]](#footnote-37) to contextualising communication,[[38]](#footnote-38) especially as social media communication can be more permanent than ephemeral. In addition to anonymity and pseudonymity, creating multiple accounts on the same platform has important social benefits.

Secondary accounts on platforms like Twitter or Instagram are often created to manage multiple, overlapping audiences and contexts by only communicating with a small group of trusted, intimate friends.[[39]](#footnote-39) The ‘Finsta’ account, a portmanteau of ‘fake’ and ‘Instagram’, is especially popular among young people, as having multiple accounts on Instagram allows them to toggle between a public-facing account with images suitable for ‘collapsed contexts’,[[40]](#footnote-40) and the alternative or Finsta for sharing more personal content with a small group of close friends’ Finstas.[[41]](#footnote-41)

Finstas, despite being labelled ‘fake’, refer only to their pseudonymous nature, and not to any calculated attempts at duplicity. Most young people use Finstas as a way to communicate a more realistic or authentic version of their daily lives.[[42]](#footnote-42) This makes Finstas a reaction to the perception of surveillance and scrutiny by peers, educators, and potential future employees, instead of an avenue for harassing and bullying others. The “malicious intent”[[43]](#footnote-43) that Facebook identifies as a key aspect in fake accounts is not usually present in a Finsta or secondary social media account.

## What identity verification is already being done in social media?

Some countries around the world have started to consider legislation aimed at requiring identity verification by social media, for example:

* In **India**, earlier in 2020, it was reported that its Cabinet approved the introduction of the Personal Data Protection Bill, which proposes that social media companies enable ‘voluntary verification’ of user accounts. These verified users will then be given a “demonstrable and visible mark of verification which is akin to biometric or physical identification which is publicly visible to all users”.[[44]](#footnote-44)
* In **Brazil**, in September 2019, a draft Bill was introduced which would require identity verification for users who create accounts on social networking platforms. The proposal would amend Brazilian internet law to require social media companies to ensure the unambiguous identification of their users by verifying their official identifications.[[45]](#footnote-45)

However, in **China**, controls on the media, including social media, are the strictest in the world. Legislation enforces real-name registration, holds companies liable for online content, requires internet chat service providers to verify the identities of users, and apparently orders telecommunication firms to bar the use of VPNs.[[46]](#footnote-46) It has also been reported that Chinese citizens now must use facial identification to sign up for internet services or receive a new mobile number.[[47]](#footnote-47)

In **South Korea**, a real name verification system for popular internet platforms, based on national identification numbers, was implemented in 2007 to reduce offensive speech, libel, and crime.[[48]](#footnote-48) The verification system was ruled unconstitutional and abandoned in 2012, as it was considered an unwarranted incursion on the liberties of South Koreans, and a threat to political and social expression.[[49]](#footnote-49) The abandonment of the verification system occurred at a time when global social media platforms like Facebook, Twitter, and YouTube were proliferating, making national boundaries on an increasingly global internet difficult to police.[[50]](#footnote-50)

From the social media companies themselves there have also been signs of being open to the concept of identity verification. On **Facebook**, if someone is locked out of their account, they can confirm their identity to regain access. “You have several different options for this”, Facebook tells users, “including photo IDs issued by the government, IDs from non-government organizations, official certificates or licenses that include your name or other physical items like a magazine subscription or a piece of mail”.[[51]](#footnote-51) Facebook has recently announced that viral posts from unverified accounts will have limited reach. That is, Facebook will reduce the distribution of that account’s viral posts, which will reduce the number of people who see it appear in their feed.[[52]](#footnote-52) In response to privacy concerns, Facebook has stated that when people upload identification documents, the documents are encrypted and then deleted within 30 days.[[53]](#footnote-53)

**Twitter**’s verification system began in 2009 after high-profile users began to be impersonated. Before the verification process was suspended, Twitter itself sought out Twitter accounts it deemed to be in the public interest – usually in music, acting, fashion, government, politics, religion, journalism, media, sports, business, or other key interest areas.[[54]](#footnote-54) From 2016, people were allowed to apply for verification themselves, rather than waiting to be prompted by the platform. Once someone was verified, a blue check mark would appear as a badge next to their username.[[55]](#footnote-55) This verification system is not widely considered successful. A 2017 controversy in which a white supremacist in the US was verified by Twitter led the company to apologise for the confusion in the verification system: “Verification was meant to authenticate identity & voice but it is interpreted as an endorsement or an indicator of importance”.[[56]](#footnote-56) It should be noted that the verified account program is currently on hold and Twitter is working on a new authentication and verification program.[[57]](#footnote-57)

No other social media companies appear to have made any policy changes relating to identity verification.

## How could online identity verification be achieved?

Several options exist for online identify verification, such a through a third-party provider, through a government agency, or by the social media provider itself.

### Third-party providers

A number of third-party information and analytics companies exist to provide identity and age verification checks on consumers, as well as credit checks and fraud assessments. Industries that use identity verification services include banking, financial services, digital businesses, travel and leisure providers, sharing economy businesses (such as ride sharing businesses and delivery services), telecommunication services, technology providers, gaming and entertainment. Assessments are often made across a range of data sources or databases, and a variety of personal information can be collected (which are outlined in the privacy policies of these companies).

### Government agency

The Digital Identity program, led by the Federal Government Digital Transformation Agency, is intended to provide Australian people and businesses a single, secure way to authenticate their identity for the purpose of accessing government services online.[[58]](#footnote-58)

This program is starting with Federal Government services, but intends to eventually include private sector and other state and local government services. The Federal Government currently requires a different login for more than 30 different digital services, such as Medicare, myTax and Centrelink. Eventually, a digital identity will be able replace these 30 different logins and make accessing government services faster and easier.

This system includes accredited service providers (for example, the Australian Tax Office through the myGov service and, as described earlier, in this paper Australia Post’s Digital iD service) and provides Australians with a single and secure way to use government services online, removing the need for the public to have to verify who they are in person at a government office. The system also includes an accredited identity exchange, run by Services Australia, which ensures the identity verification provider cannot see what online service the user is accessing, and the online service cannot see someone’s personal information. The scheme is completely voluntary.

The Digital Transformation Agency has been developing – in close cooperation with industry, government, academia and privacy experts – a system called the Trusted Digital Identity Framework (TDIF) which would enable the use of identity credentials from one service provider to establish their identity at another. Identity providers wishing to participate in the Digital Identity system must meet ‘strict privacy and security requirements’ set out in the TDIF. The TDIF also defines a hierarchy of identity proofing levels, namely:[[59]](#footnote-59)

* **Level 1** is used when no identity verification is needed or when a very low level of confidence in the claimed Identity is needed. This level supports self-asserted identity (I am who I say I am) or pseudonymous Identity. The intended use of Identity Proofing Level 1 is for services where the risks of not undertaking identity verification will have a negligible consequence to the Individual or the service, for example, to pay a parking infringement or obtain a fishing licence.
* **Level 1 Plus** is used when a low level of confidence in the claimed identity is needed. This requires one identity document to verify someone’s claim to an existing identity. The intended use of Identity Proofing Level 1 plus is for services where the risks of getting identity verification wrong will have minor consequences to the Individual or the service, for example, the provision of loyalty cards.
* **Level 2** is used when a low-medium level of confidence in the claimed identity is needed. This requires two or more Identity Documents to verify someone’s claim to an existing identity. The intended use of Identity Proofing Level 2 is for services where the risks of getting identity verification wrong will have moderate consequences to the Individual or the service, for example, the provision of utility services. An Identity Proofing Level 2 identity check is sometimes referred to as a ‘100-point check’.
* **Level 2 Plus** is used when a medium level of confidence in the claimed identity is needed. This requires two or more Identity Documents to verify someone’s claim to an existing identity and requires the Binding Objective to be met. The intended use of Identity Proofing Level 2 plus is for services where the risks of getting identity verification wrong will have moderate-high consequences to the Individual or the service, for example, undertaking large financial transactions.
* **Level 3** is used when a high level of confidence in the claimed identity is needed. This requires three or more Identity Documents to verify someone’s claim to an existing identity and requires the Binding Objective to be met. The intended use of Identity proofing Level 3 is for services where the risks of getting identity verification wrong will have high consequences to the Individual or the service, for example, access to welfare and related government services.
* **Level 4** is used when a very high level of confidence in the claimed identity is needed. This requires four or more Identity Documents to verify someone’s claim to an existing identity and the individual claiming the identity must attend an in-person interview as well as meet the requirements of Identity Proofing Level 3. The intended use of Identity Proofing Level 4 is for services where the risks of getting identity verification wrong will have a very high consequence to the Individual or the service, for example, the issuance of government-issued documents such as an Australian passport.

While the TDIF is primarily for Government services, it is also freely available as a framework for all Australian businesses today as a reference for best practice and how to verify identity online.[[60]](#footnote-60) The Digital Transformation Agency would need legislative authority for the program to connect directly to services in the private sector, including social media platforms.

### Social media providers

As mentioned above, Facebook already limits the reach of any posts from accounts that have not undertaken identity verification. Similarly, any social media company could require in-house identity verification before an account is activated. The Queensland Anti-Cyberbullying Taskforce noted that there would be privacy risks given the challenges social media companies have already experienced with data security. Identity verification systems raise questions about access to personal and sensitive data. Any regulations considered should therefore ensure that these systems do not reuse collected data for any other purposes.

## The benefits and disadvantages of online identity verification

While identity verification is not necessarily required for commercial industry, businesses in every industry today are moving to digital models. From banking, to shopping, to travel, companies are using digital infrastructure to connect people with what they want and need right now. While digital identity verification may be used for banking and travel purposes, for online shopping purposes, businesses generally only require proof of payment for good and services and not necessarily verification that a person is who they say they are.

**Benefits of online identity verification**

Noting the previous section, ‘Would identity verification help reduce cyberbullying’ and the efforts of other countries to implement identity verification, requiring social media companies to verify identity may have benefits associated with cyberbullying by reducing the number of under-age children using social media and reducing the number of fake accounts often used to perpetrate cyberbullying. However, overall there is limited evidence to support this claim.

**Disadvantages of online identity verification**

There appears to be three main disadvantages to identity verification:

1. **Increased costs for social media companies:**[[61]](#footnote-61) it will cost social media companies more in both time and effort to ensure that accounts are identity verified.
2. **The use of social media identity data:** social media companies, particularly if identity is verified by the social media provider itself rather than through a third-party provider or a government agency, will have access to large amount of personal data. This data has been supplied by the user specifically for identity verification and not for any other purpose. However, there is a risk the data may be used inappropriately, for example, to improve the social media companies’ ability to personalise targeting of advertisements and marketing.
3. **Risks to privacy:** including risks of hacking, location disclosure, and third-party personal information disclosure. Regardless of whether identity is verified through a third-party provider, a government agency, or by the social media provider itself it will be vital that standards be developed that should specify minimum requirements for privacy, safety, security, data handling, usability, accessibility, and auditing of identity verification providers.

It is important to note that identity verification does not equate to the user’s identity being known by everyone. After a user’s identity is verified the user’s name as seen by other users could still be something anonymous as we often see today (like hotdog54, cooldude23, etc). Thus, a worker who does not want their employer to know of their social activities, or a victim of domestic and family violence who does not want the perpetrator to know what they are doing, could still have anonymity.

The difference is that anyone who is engaging in cyberbullying, or any of the other behaviours listed earlier in this section, would not be anonymous to the appropriate authorities.

# Further areas for consideration

Based on the available academic scholarship on identity verification for social media, this report suggests the following points for consideration.

1. **Australian citizens are unlikely to welcome further digital surveillance.** According to the Digital Rights Watch, government power over the digital lives of Australians needs to be kept in check to maintain human rights online.[[62]](#footnote-62) Social media users are already aware of their content being under scrutiny by their extended social network, and self-monitor their social media posts as a result,[[63]](#footnote-63) even without having their social media accounts formally linked with government-issued identification documents.
2. **Moving to a system of verifying identities on social media must be done with respect for the autonomy and freedom of Australians.** According to communications scholar Kelly A Gates, “the most stable, peaceful societies are not societies in which everyone is identifiable all the time everywhere they go. Instead, they are societies in which social and cultural differences are respected, and people have a healthy measure of autonomy and control over their own lives”.[[64]](#footnote-64) If identity verification for social media were to be implemented in Australia, this should involve actively avoiding ‘scope creep’ or constantly expanding government surveillance. For example, submitted identity documents could be deleted after 30 days as Facebook currently does, to mitigate privacy and security concerns,[[65]](#footnote-65) and social media users should still be allowed to create pseudonymous and multiple accounts on platforms so they can effectively compartmentalise their identities.[[66]](#footnote-66)
3. **Taking harassment and bullying on social media seriously must involve effective reporting and moderation systems.** These systems are currently complex, and known to exploit vulnerable populations. Australian digital governance scholar Nicolas Suzor argues that the internet does not create, but instead amplifies, existing discrimination and harassment already disproportionately experienced by women and minorities. Social media reporting systems need improvement, Suzor claims.[[67]](#footnote-67) In this context, it is worth asking what would happen when someone engages in social media harassment or bullying with a verified account. Who is expected to monitor and follow up with reports of bullying, and what standards for identifying and assessing bullying will apply?
4. **If age verification means children under 13 are no longer able to access social media platforms like Facebook, consider meaningful alternatives.** Research into virtual worlds designed especially for children, such as Club Penguin, shows that these platforms provide a motivating context for developing digital literacy skills,[[68]](#footnote-68) and allows them to playfully experiment with identity and socialising with peers.[[69]](#footnote-69) While the Facebook Messenger Kids app has been criticised for collecting data about children, and potentially locking them into the Facebook ecosystem early, it also provides parental controls for messaging.[[70]](#footnote-70)

# Conclusions

From the material examined, it is considered both technologically and procedurally possible for social media companies to implement identity verification, although the points raised in this paper ought to be considered to ensure identity verification is carried out with respect for the digital rights of Australians.

It should be noted that no literature was found indicating that any individual states within a country had attempted enacting any legislation around either age verification or identity verification.

If identify verification for social media companies were to be pursued further, a national focus would be needed to ensure that telecommunication firms deny service to any companies not complying with regulations.

In Australia, the regulation of the internet is generally a Federal Government responsibility and the States and Territories have limited scope under the Constitution of Australia to regulate in this space. Under s 51(v) of the Constitution of Australia, the Commonwealth has power in respect of “postal, telegraphic, telephonic and other like services”. The phrase “other like services” indicates the power was designed to cover new technological developments, thus giving constitutional power to regulate in this space to the Commonwealth. Therefore, it is considered that enacting any identity verification legislation for social media would be best accomplished at the federal level.

As mentioned earlier in this paper, the House of Representatives Standing Committee on Social Policy and Legal Affairs tabled its report in March 2020 titled *Protecting the age of innocence: Report of the inquiry into age verification for online wagering and online pornography.*[[71]](#footnote-71) While there has been no Federal Government response to date,[[72]](#footnote-72) the suggestions outlined below in relation to identity verification are in alignment with this report’s recommendations in relation to age verification.

As a dedicated office with relevant expertise, industry knowledge, and an understanding of the broader issues associated with online safety, it is considered that the eSafety Commissioner would be best placed to progress identity verification in Australia, should this be pursued further.

The Queensland Government could advocate that the Federal Government work with the eSafety Commissioner to develop a roadmap to examine implementing mandatory online identity verification for social media, setting out:

1. a suitable legislative and regulatory framework, including appropriate standards and accountability measures relating to data protection, privacy, safety and dignity for all users, but especially ensuring children and young people are adequately protected
2. a program of consultation with community, industry, and government stakeholders
3. an implementation plan to support an online identity verification trial.

The eSafety Commissioner could consult with the Digital Transformation Agency in relation to the development of appropriate technical standards for identity verification and an identity verification exchange to ensure that any regime for identity verification for social media leverages these more general capabilities.

Further, the Digital Transformation Agency could – in consultation with industry, including private identity verification providers, and members of the public – develop standards (or modify existing standards) for online identity verification in relation to social media. These standards could specify minimum requirements for privacy, safety, security, data handling, usability, accessibility, and auditing of identity verification providers.

The Digital Transformation Agency could also extend its Digital Identity program to include an identity verification exchange for the purpose of third-party online identity verification and be granted the legislative authority for the program to connect directly to services in the private sector.

However, it is important to note that while verifying online and digital identity is possible, the recent difficulties in mandating this, as experienced by the United Kingdom in attempting to introduce the nationwide age verification system for online pornography, should not be underestimated.

While limited, the experience of other international efforts highlights the technical and privacy challenges in mandating identity verification and its efficacy. The biggest two obstacles will be: a) ensuring that data has been supplied by the user specifically for identity verification is not for any other purpose; and b) minimising the risks to privacy, such as the risks of hacking, location disclosure, and third-party personal information disclosure.

1. Queensland Anti-Cyberbullying Taskforce, September 2018, Adjust our Settings: A community approach to address cyberbullying among children and young people in Queensland, p.5. <https://campaigns.premiers.qld.gov.au/antibullying/taskforce/assets/anti-cyberbullying-taskforce-final-report.pdf> [↑](#footnote-ref-1)
2. Ibid, p.7. [↑](#footnote-ref-2)
3. Ibid, p.66. [↑](#footnote-ref-3)
4. Queensland Anti-Cyberbullying Taskforce, September 2018, Adjust our Settings: A community approach to address cyberbullying among children and young people in Queensland, p.19. <https://campaigns.premiers.qld.gov.au/antibullying/taskforce/assets/anti-cyberbullying-taskforce-final-report.pdf> [↑](#footnote-ref-4)
5. Search Engine Journal, 3 February 2020, The 7 Biggest Social Media Sites in 2020. <https://www.searchenginejournal.com/social-media/biggest-social-media-sites/#close> [↑](#footnote-ref-5)
6. Omnicore 2020, YouTube by the Numbers: States, Demographics & Fun Facts, <https://www.omnicoreagency.com/youtube-statistics/> [↑](#footnote-ref-6)
7. Adobe Spark, 2020, The 7 Top Social Media Sites You Need to Care About in 2020. <https://spark.adobe.com/make/learn/top-social-media-sites/> [↑](#footnote-ref-7)
8. We Are Social, 12 February 2020, Digital 2020 in Australia: 1 in 3 Minutes Online are Spent on Social, https://wearesocial.com/au/blog/2020/02/digital-2020-in-australia-analysis [↑](#footnote-ref-8)
9. Roy Morgan, 16 April 2020, Facebook and YouTube strong across all Generations but Pinterest, Instagram and TikTok have important user bases, http://www.roymorgan.com/findings/8373-social-media-demographics-march-2020-202004140629. [↑](#footnote-ref-9)
10. Australian Psychological Society 2017, Digital Me – a survey exploring the effect of social media and

    digital technology on Australians’ wellbeing. <https://www.qfcc.qld.gov.au/digital-me-survey-exploring-effect-social-media-and-digital-technology-australians-wellbeing> [↑](#footnote-ref-10)
11. Office of the eSafety Commissioner, 3 May 2018, State of Play – youth, kids and digital dangers. <https://www.esafety.gov.au/sites/default/files/2019-10/State%20of%20Play%20-%20Youth%20kids%20and%20digital%20dangers.pdf> [↑](#footnote-ref-11)
12. Australian Parenting Website, Social media benefits and risks: children and teenagers. <https://raisingchildren.net.au/teens/entertainment-technology/digital-life/social-media>

    internetmatters.org, Social media benefits. <https://www.internetmatters.org/resources/social-media-advice-hub/social-media-benefits/>

    verywell family, Surprising Ways Your Teen Benefits From Social Media. <https://www.verywellfamily.com/benefits-of-social-media-4067431>

    common sense media, 5 reasons You Don’t Need to Worry About Kids and Social Media. <https://www.commonsensemedia.org/blog/5-reasons-you-dont-need-to-worry-about-kids-and-social-media> [↑](#footnote-ref-12)
13. Echeburua, E and de Corral, P, 2010, Addiction to new technologies and to online social networking in young people: A new challenge, *Adicciones*, vol. 22, no. 2, pp. 91-95. [↑](#footnote-ref-13)
14. Australian Parenting Website, Social media benefits and risks: children and teenagers. <https://raisingchildren.net.au/teens/entertainment-technology/digital-life/social-media>

    kids help line, Social media and safety. <https://kidshelpline.com.au/parents/issues/social-media-and-safety>

    whistle out, Kids on social media: The dangers parents need to know. <https://www.whistleout.com.au/MobilePhones/Guides/Parenting-Dangers-and-Risks-of-Social-Media-for-Kids> [↑](#footnote-ref-14)
15. Campbell, Marilyn, Spears, Barbara, Slee, Phillip, Butler, Des, & Kift, Sally (2012) Victims' perceptions of traditional and cyberbullying, and the psychosocial correlates of their victimisation. Emotional and Behavioural Difficulties, 17(3-4), pp. 389-401. <https://eprints.qut.edu.au/53597/> [↑](#footnote-ref-15)
16. Hinduja S, Patchin JW. 2010. ‘Bullying, cyberbullying, and suicide’. Arch Suicide Res. <https://www.ncbi.nlm.nih.gov/pubmed/20658375> [↑](#footnote-ref-16)
17. Australia Post, Digital ID. <https://www.digitalid.com/business> [↑](#footnote-ref-17)
18. Australia Post, Digital ID. <https://www.digitalid.com/personal> [↑](#footnote-ref-18)
19. Huffington Post, 10 August 2014, 3 Reasons Why Social Media Age Restrictions Matter. <https://www.huffingtonpost.com/diana-graber/3-reasons-why-social-media-age-restrictions-matter_b_5935924.html> [↑](#footnote-ref-19)
20. Federal Trade Commission 1998, Children's Online Privacy Protection Rule, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule. [↑](#footnote-ref-20)
21. UK Public General Acts 2017, Digital Economy Act 2017, https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted. [↑](#footnote-ref-21)
22. The Guardian, 17 Oct 2019, UK drops plans for online pornography age verification system. <https://www.theguardian.com/culture/2019/oct/16/uk-drops-plans-for-online-pornography-age-verification-system> [↑](#footnote-ref-22)
23. Politico, 9 July 2020, France to introduce controversial age verification system for adult websites. <https://www.politico.eu/article/france-to-introduce-controversial-age-verification-system-for-adult-pornography-websites/> [↑](#footnote-ref-23)
24. Institut Montaigne blog, 25 June 2020, Age Verification Online: What is at stake? <https://www.institutmontaigne.org/en/blog/age-verification-online-what-stake> [↑](#footnote-ref-24)
25. House of Representatives Standing Committee on Social Policy and Legal Affairs, February 2020, Protecting the age of innocence: Report of the inquiry into age verification of online wagering and online pornography, page vii. <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report> [↑](#footnote-ref-25)
26. Ibid, p.66. [↑](#footnote-ref-26)
27. Ibid, p.66. [↑](#footnote-ref-27)
28. Srivastava, A, Gamble, R & Boey, J 2013, ‘Cyberbullying in Australia: Clarifying the Problem, Considering the Solutions’, *International Journal of Children's Rights*, vol. 21, pp. 25-45; Bartlett, CP 2015, ‘Anonymously Hurting Others Online: The Effect of Anonymity on Cyberbullying Frequency’, *Psychology of Popular Media Culture*, vol. 4, no. 2, pp. 70-79; Moore, MJ, Nakano, T, Enomoto, A & Suda, T 2012, ‘Anonymity and Roles Associated with Aggressive Posts in an Online Forum’, *Computers in Human Behavior*, vol. 28, no. 3, pp. 861-867. [↑](#footnote-ref-28)
29. Entrepreneur, 11 April 2019, How Digital Identification Can Curb Fake Social Media Accounts. <https://www.entrepreneur.com/article/332081> [↑](#footnote-ref-29)
30. Rösner, L & Krämer, NC 2016, 'Verbal Venting in the Social Web: Effects of Anonymity and Group Norms on Aggressive Language Use in Online Comments', *Social Media + Society*, vol. 2, July-September, pp. 1-13. [↑](#footnote-ref-30)
31. Carlson, BL, Jones, LV, Harris, M, Quezada, N & Frazer, R 2017, 'Trauma, Shared Recognition and Indigenous Resistance on Social Media', *Australasian Journal of Information Systems*, vol. 21, pp. 1-18. [↑](#footnote-ref-31)
32. NATO Strategic Command Centre of Excellence, 5 December 2019, How Social Media Companies are Failing to Combat Inauthentic Behaviour Online. <https://www.stratcomcoe.org/how-social-media-companies-are-failing-combat-inauthentic-behaviour-online> [↑](#footnote-ref-32)
33. Statista, 3 Feb 2020, 16% of All Facebook Accounts Are Fake or Duplicates. <https://www.statista.com/chart/20685/duplicate-and-false-facebook-accounts/#:~:text=The%20social%20network%20estimates%20the,about%20137%20million%20user%20profiles).> [↑](#footnote-ref-33)
34. Facebook Transparency Report, <https://transparency.facebook.com/> [↑](#footnote-ref-34)
35. Forbes, 22 Feb 2018, Is It Time To Require Identity Verification For Everyone Using Social Media? <https://www.forbes.com/sites/willburns/2018/02/22/is-it-time-to-require-identity-verification-for-everyone-using-social-media/#70fc43218683> [↑](#footnote-ref-35)
36. Marwick, A 2013, ‘Online Identity’, pp. 355-364 in J Hartley, J Burgess & A Bruns (eds), *A Companion to New Media Dynamics*, Wiley-Blackwell, Chichester; Schmidt, J-H 2013, 'Practices of Networked Identity', pp. 365–374 in J Hartley, J Burgess & A Bruns (eds), *A Companion to New Media Dynamics*, Wiley-Blackwell, Chichester. [↑](#footnote-ref-36)
37. Hogan, B 2013, ‘Pseudonyms and the Rise of the Real-Name Web’, pp. 290-307 in *A Companion to New Media Dynamics*, J Hartley, J Burgess, A Bruns (eds), Wiley-Blackwell, Chichester. [↑](#footnote-ref-37)
38. van der Nagel, E & Frith, J 2015, 'Anonymity, Pseudonymity, and the Agency of Online Identity: Examining the Social Practices of r/Gonewild', *First Monday*, vol. 20, no. 3, https://firstmonday.org/ojs/index.php/fm/article/view/5615. [↑](#footnote-ref-38)
39. van der Nagel, E 2018, 'Alts and Automediality: Compartmentalising the Self through Multiple Social Media Profiles', *M/C Journal: A Journal of Media and Culture*, vol. 21, no. 2, http://journal.media-culture.org.au/index.php/mcjournal/article/view/1379. [↑](#footnote-ref-39)
40. Marwick, A & boyd, d 2011, ‘I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience’, *New Media & Society*, vol. 13, no. 1, pp. 114-133. [↑](#footnote-ref-40)
41. Kang, J & Wei, L 2020, 'Let Me Be at My Funniest: Instagram Users’ Motivations for Using Finsta (a.k.a., fake Instagram)', *The Social Science Journal*, vol. 57, no. 1, pp. 58–71. [↑](#footnote-ref-41)
42. Duffy, BE & Chan, NK 2019, '“You Never Really Know Who's Looking": Imagined Surveillance Across Social Media Platforms', *New Media & Society*, vol. 21, no. 1, pp. 119–138. [↑](#footnote-ref-42)
43. Facebook Transparency Report, <https://transparency.facebook.com/> [↑](#footnote-ref-43)
44. Gadgets 360, 17 Jan 2020, Social Media Rules May Make User ID Verification Mandatory. <https://gadgets.ndtv.com/social-networking/news/social-media-rules-may-make-user-id-verification-mandatory-report-2165553> [↑](#footnote-ref-44)
45. Lexology, 11 Nov 2019, Brazil - Draft Bill requires social networks to verify the identity of their users using official IDs. <https://www.lexology.com/library/detail.aspx?g=e575ad40-3b6f-49f4-a9c4-c2b39400c95d> [↑](#footnote-ref-45)
46. eSafety Commissioner, November 2019, “Inquiry into age verification for online wagering and online pornography”, Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs, page 23. <https://www.aph.gov.au/DocumentStore.ashx?id=2c35bb2c-4a68-428b-af67-cf05ff17052e&subId=673265> [↑](#footnote-ref-46)
47. Business Insider Australia, 11 Oct 2019, Chinese government forces people to scan their face before they can use internet as surveillance efforts mount. <https://www.businessinsider.com.au/china-to-require-facial-id-for-internet-and-mobile-services-2019-10?r=US&IR=T> [↑](#footnote-ref-47)
48. Cho, D 2013, ‘Real Name Verification Law on the Internet: A Poison or Cure for Privacy?’, pp. 239-261 in B Schneier (ed), *Economics of Information Security and Privacy III*, Springer, New York. [↑](#footnote-ref-48)
49. Leitner, J 2009, ‘Identifying the Problem: Korea’s Initial Experience with Mandatory Real Name Verification on Internet Portals’, *Journal of Korean Law*, vol. 9, no. 1, pp. 83-108. [↑](#footnote-ref-49)
50. Kim, K 2016, ‘Korean Internet and ‘Real Name’ Verification Requirement’, *Korea University Law Review*, vol. 20, pp. 87-104. [↑](#footnote-ref-50)
51. Confirm Your Identity with Facebook, 2020, https://www.facebook.com/help/contact/183000765122339. [↑](#footnote-ref-51)
52. The Verge, 28 May 2020, Facebook will start verifying the identities of accounts that keep going viral. <https://www.theverge.com/2020/5/28/21273784/facebook-id-verification-suspicious-accounts-viral-misinformation> [↑](#footnote-ref-52)
53. The Conversation, 9 May 2019, Facebook wants to combat fake news with ID checks – with ‘grave implications’ for our privacy. <https://theconversation.com/facebook-wants-to-combat-fake-news-with-id-checks-with-grave-implications-for-our-privacy-116569> [↑](#footnote-ref-53)
54. Twitter Help Centre, About verified accounts. <https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts> [↑](#footnote-ref-54)
55. Hearn, A 2017, ‘Verified: Self-Presentation, Identity Management, and Selfhood in the Age of Big Data’, *Popular Communication*, vol. 15, no. 2, pp. 62-77. [↑](#footnote-ref-55)
56. @TwitterSupport, 10 November 2017, Verification, https://twitter.com/TwitterSupport/status/928654369771356162. [↑](#footnote-ref-56)
57. Twitter Support. <https://twitter.com/TwitterSupport/status/930926225517719552> [↑](#footnote-ref-57)
58. Digital Transformation Agency, ‘Digital Identity’. <https://www.dta.gov.au/our-projects/digital-identity> [↑](#footnote-ref-58)
59. Digital Transformation Agency, ‘Trusted Digital Identity Framework’. <https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework> [↑](#footnote-ref-59)
60. Mr Peter Alexander, Chief Digital Officer, Digital Transformation Agency, Committee Hansard, Canberra, 6 December 2019, p. 41. [↑](#footnote-ref-60)
61. Suzor, NP 2019, *Lawless: The Secret Rules that Govern Our Digital Lives*, Cambridge University Press, Cambridge, p. 15. [↑](#footnote-ref-61)
62. Digital Rights Watch 2018, State of Digital Rights,

    https://digitalrightswatch.org.au/wp-content/uploads/2018/05/State-of-Digital-Rights-Web.pdf. [↑](#footnote-ref-62)
63. Marwick, AE 2012, ‘The Public Domain: Social Surveillance in Everyday Life’, *Surveillance & Society*, vol. 9, no. 4, pp. 378-393. [↑](#footnote-ref-63)
64. Gates, KA 2011, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, New York University Press, New York. [↑](#footnote-ref-64)
65. The Conversation, 9 May 2019, Facebook wants to combat fake news with ID checks – with ‘grave implications’ for our privacy. https://theconversation.com/facebook-wants-to-combat-fake-news-with-id-checks-with-grave-implications-for-our-privacy-116569. [↑](#footnote-ref-65)
66. van der Nagel, E 2018, 'Alts and Automediality: Compartmentalising the Self through Multiple Social Media Profiles', *M/C Journal: A Journal of Media and Culture*, vol. 21, no. 2, http://journal.media-culture.org.au/index.php/mcjournal/article/view/1379. [↑](#footnote-ref-66)
67. Suzor, NP 2019, *Lawless: The Secret Rules that Govern Our Digital Lives*, Cambridge University Press, Cambridge. [↑](#footnote-ref-67)
68. Marsh, J 2014, 'Purposes for literacy in children's use of the online virtual world Club Penguin', *Journal of Research in Reading*, vol. 37, no. 2, pp. 179-195. [↑](#footnote-ref-68)
69. Burley, D 2010, 'Penguin Life: A Case Study of One Tween's Experiences inside Club Penguin', *Journal of Virtual Worlds Research*, vol. 3, no. 2, pp. 3-13. [↑](#footnote-ref-69)
70. Biggs, T, 24 April 2020, Privacy advocates raise concerns as Facebook's chat for kids rolls out, *Sydney Morning Herald*,

    https://www.smh.com.au/technology/privacy-advocates-raise-concerns-as-facebook-s-chat-for-kids-rolls-out-20200423-p54mkg.html. [↑](#footnote-ref-70)
71. House of Representatives Standing Committee on Social Policy and Legal Affairs, February 2020, Protecting the age of innocence: Report of the inquiry into age verification of online wagering and online pornography. <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report> [↑](#footnote-ref-71)
72. For updates on any response see <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Completed_inquiries> [↑](#footnote-ref-72)