Anonymity and identity shielding online - Tech trends position statement

Definition

Anonymity and identity shielding allow a user to hide or disguise their identifying information online. While this protects their privacy, it can make it difficult to hold them responsible for what they say and do online.

Anonymous communication is seen by many as a cornerstone of promoting freedom of speech, expression and privacy on the internet, but it can also be misused to control and abuse people

Background

A user can hide or disguise their identifying information, such as their real name, age, location and data use, through:

- total anonymity – not revealing any identifying information about themselves
- partial anonymity – only revealing their identifying information to a limited audience that shields it from the general public.

There are various ways for a user to hide or disguise their identifying information.

Technical approaches to anonymity include software, browsers and encrypted or decentralised platforms. Examples include virtual private networks that mask the user's location and device details (IP address), anonymising processes that conceal the link between a message and the sender, and end-to-end encryption that allows only a sender and recipient to decode digital content.

Simpler approaches involve taking on a fictional identity. Examples include using a false name (a 'pseudonym' or an 'alias'), a virtual representation (an 'avatar'), or a fake profile. Fictional identities may be used legitimately as a means of protecting privacy, or they may be used deceptively to trick platform hosts and other users.

Positive use cases

There are a number of good reasons for anonymity or shielding one's identity online.

One is to limit or control how personal data is collected and stored, as well as who can access and use it. This helps prevent security breaches, surveillance and intrusive web-tracking. For example, features such as cookies and facial recognition technologies streamline the user experience, making it easy to access digital devices and platforms and find the most relevant information, but they can also be used by online services to map the habits of individuals, such as their spending patterns, then target them with advertising.

Another reason for anonymity and identity shielding is to protect users from unwanted contact. For example, eSafety encourages children only to use their given name, a nickname or an avatar online instead of full real name. This makes it more difficult for sexual predators and scammers to interact with them. It can also be important to remain anonymous or shield identifying information for individuals experiencing domestic and family violence, to make it more difficult for stalking or harassment to be perpetuated through technology.

In addition, anonymity and identity shielding also enables people to freely engage online without feeling inhibited. For example, it can allow people who are same sex attracted, intersex or gender diverse to explore their identity and to talk openly about their sexuality free from being 'outed' to their family and friends or harassed. Anonymity also allows people to freely express ideas and critique people in power without risking retaliation or life-threatening consequences.

Risks

Despite its positive uses, anonymity and identity shielding can also spur on harmful behaviours and generate new forms of harm, particularly against at-risk individuals and communities.

Anonymity is one of several factors that have been highlighted by our own investigations as a tactic used by those who seek to harm or abuse others online. There are two main reasons for this.

Firstly, being anonymous can make perpetrators feel uninhibited by the usual social standards of behaviour. By hiding their real identity or using fake profiles they can act without the fear of being judged for their actions or punished.

Secondly, being able to hide their real identity allows individuals and crime syndicates to pretend to be someone else and use that as a way to exploit others.

- The ease with which anonymous, fake, imposter and impersonator accounts can be generated is a contributing factor to cyberbullying of children and adult cyber abuse, as reflected in a significant number of the complaints we receive through our reporting schemes.
- Most image-based abuse complaints to eSafety relate to anonymous accounts on social media platforms. Image-based abuse means sharing or threatening to share an intimate image or video without the consent of the person shown. It includes sextortion, when scammers demand money or more intimate images.
- Most investigations into child sexual abuse material involve individuals posting the content online anonymously. These investigations have shown that content contributors will go to great lengths to remain anonymous, often using one or more anonymising security measure to hide their identities.
- Sexual predators and scammers also commonly use anonymous, fake, imposter and impersonator accounts to lure victims and gain their trust. For example, a sexual predator may use an avatar in a game to pretend they are the same age and gender as a child so they can become a fake friend and groom them for sexual interaction. In catfishing cases, scammers often create a fake profile and pretend to have a personal history and characteristics that are attractive to the victim, so they are more likely to engage online and not be suspicious while in the relationship.
- Some chatrooms and message board sites are specifically created for anonymous communication, allowing the fast and wide spread of conspiracy theories, discriminatory commentary and illegal and harmful materials, and even inciting acts of abuse, violence and terrorism.

Interaction with an anonymous account online can be very distressing for victims who are targeted by abuse. The fear that the perpetrator can continue to target the victim using another anonymous or fake account adds to the harm. For victims, anonymity can create barriers to reporting. This is because perpetrators using imposter or fake accounts are not easily identifiable. These fake accounts can be quickly discarded and replaced with new anonymous accounts, making techniques such as blocking and muting ineffective.

It is very difficult for regulators and law enforcement to identify and prosecute individuals and crime syndicates using fake accounts. It also makes it almost impossible for social media services and other users to deal with abusers breaching the terms of service, through strategies such as blocking and suspension, as well as preventing, detecting and removing multiple accounts operated by one user.

While conflict, harassment and targeted abuse are social and cultural problems, the role that anonymity plays in facilitating antisocial and illegal behaviour has been a growing cause for concern. However, it is important to note that preventing or limiting anonymity and identity shielding online would not put a stop to all online abuse, and that online abuse and hate speech are not always committed by anonymous or fake account holders.

Nevertheless, more can be done to ensure anonymity is not used to allow harms to freely occur. Steps can be taken by social media platforms to verify accounts before users start to operate them, or take down accounts that violate the terms of service and prevent them from resurfacing.

A balance is needed, where the misuse of anonymity and identity shielding is restricted without removing any of the legitimate benefits.

Current industry practice

A variety of mechanisms are used by industry to authenticate online account holders.

Many platforms and services require users to provide an email address or phone number in order to sign up, with some requiring people to use their real names (though real name policies have been heavily criticised and have been deemed illegal in some jurisdictions).

Two-factor and multi-factor authentication are also becoming more common, with users having to provide multiple credentials before being able to register or access an account. However, this requirement tends to be only for users who have already violated the terms service and want to access the platform again.

More rigorous verification processes are used by a few services:

- requesting users provide personal identifying information (such as a driver licence, birth certificate or passport)
- cross-referencing information provided with official public databases (such as driver licences or postal address files, telephone records, electoral registers or basic credit data)
- using third-party identity validation providers for verification purposes.

There have been growing calls for digital platforms and services to verify all social media accounts. This would be in the hope that regulators and law enforcement would be able to identify perpetrators of serious harm and the prosecution of those account holders would then act as a deterrent for other harmful online behaviour.

Verification does not necessarily require the service to know or control identifying information for its users, it can simply allow the service to access the information if it needs to take steps to stop abuse or prevent a user from repeatedly setting up new accounts.

Concepts such as ‘digital licence plates’, blockchain-based identity management systems and digital signatures are also being raised as pathways forward in authenticating users in digital environments.

What is clear is that stronger and more transparent identity-related policies are needed on most digital platforms. But there are no easy or quick-fix solutions – in many ways, identity issues present challenges across the entire online ecosystem. Care must be taken to balance the rights of users and ensure that solutions are evidence-based and subject to independent and objective scrutiny.

Recent coverage

There has been significant media coverage of online harassment and trolling by anonymous account holders. The examples below highlight some prominent cases reported in the Australian media, however it is important to note that online abuse can, and does, impact anyone.

- In 2020, Australian comedian Magda Szubanski experienced coordinated online abuse after appearing in a commercial encouraging people to wear masks to help contain the spread of COVID-19 – much of the abuse came from anonymous users.

- TV presenter Erin Molan also publicly shared her experience of more than a decade of online abuse, including from fake and impersonator accounts.
- There has been extensive media coverage on the spread of hate speech and misinformation on anonymous chatroom and message board sites.

eSafety approach

eSafety recognises that anonymous and fake account holders can create and spread online abuse. We take a number of approaches to preventing and dealing with the potential harms:

- We work with individuals and industry to raise awareness about the risks related to anonymous and fake accounts, helping users to protect their identity and personal information, make ethical choices about their behaviour and respond to harms.
- We support victims who have reported abuse from anonymous or fake accounts, including:
  - alerting social media services to accounts that have been misused to target victims
  - assisting with the removal of content and accounts
  - referral to police if appropriate
  - referral to external counselling and support services.
- We encourage proactive change through eSafety's Safety by Design initiative, which helps industry to embed safety and risk management into their products. This includes providing advice to industry on:
  - identifying, addressing and responding to fake, imposter or impersonator accounts
  - preventing known techniques used by perpetrators to target and abuse others
  - advising on steps to authenticate and validate user identities.

Advice for dealing with online abuse from anonymous or fake accounts

If someone seriously abuses, harasses, intimidates or threatens you, or someone in your care, there are several steps you can take:

- **Collect and preserve evidence**, using screenshots or similar methods, unless it shows nude or sexual content of someone under 18 years old.
- **Report to the platform** where the abuse or threats are occurring – The eSafety Guide provides the relevant links for many popular platforms and services.
- **Report to eSafety** – we can help remove serious cyberbullying, image-based abuse and illegal or harmful content online.
- **Block unwanted contact** – The eSafety Guide provides many of these links.
- **Seek further support** from an expert counselling service.

If you suspect online child sexual abuse or grooming by a sexual predator report it straightaway – even if it's an anonymous or fake account – to the Australian Centre to Counter Child Exploitation via the 'Report Abuse' button on accce.gov.au/report. Or you can report it anonymously to Crime Stoppers on 1800 333 000 or at crimestoppers.com.au.

And remember, if you or someone you know is at serious risk of immediate harm **call Triple Zero (000)**.

How to reach us

General enquiries: enquiries@esafety.gov.au
Subscribe: esafety.gov.au/subscribe

Social media: twitter.com/esafetyoffice
Media enquiries: media@esafety.gov.au