The Corrosive Effect of Perfect Privacy and Perfect Anonymity

How Over-Reliance on a Qualified Human Right Can Negatively Impact Other, Absolute, Human Rights

Introduction

In an increasingly digital world, the ideals of perfect privacy and perfect anonymity hold great appeal to many. The promise of being fully shielded from surveillance or identification attracts many who seek to protect personal freedoms and expression. The justification given often refers to the potentially chilling effect of surveillance, possibly in reference to the writings about the concept of the panopticon that Bentham espoused, but that was subsequently critiqued by Foucault and others[1].

However, whilst these ideals have legitimate interest, their unqualified application can have deeply corrosive effects on society, especially concerning crime and online harms that disproportionately affect vulnerable groups like children.

Perfect privacy means that no entity can access any personal data or communications without explicit permission. Perfect anonymity ensures users cannot be traced or identified in any context. Taken together, these conditions create a digital environment where illicit behaviour can thrive unchecked by accountability.

The global context reveals a complex landscape where striking a balance between privacy rights and safety is an ongoing challenge with significant societal implications. In particular, consideration should be given to the risk that absolute privacy (a qualified human right) could negatively impact other, absolute, human rights.

[1] https://www.ebsco.com/research-starters/history/panopticon

Crime and Law Enforcement Challenges

One of the foremost consequences is the empowerment of criminals. When criminals operate behind impenetrable privacy layers and anonymity, law enforcement agencies face significant challenges in investigating and prosecuting offences. extremely difficult, delaying justice and allowing crime to proliferate.

Criminals exploit encrypted communication channels and anonymous platforms to conduct drug trafficking, human trafficking, cyber-attacks, and fraud with reduced risk of detection. For instance, global efforts to combat cybercrime face delays when criminals hide behind unbreakable anonymity, frustrating investigations and prosecutions.

Without the ability to identify and gather crucial digital evidence, security agencies are forced to rely on outdated or less effective methods. This gap compromises public safety and undermines trust in the legal systems designed to protect communities.

International Legal Perspectives

Globally, nations adopt varied approaches to privacy and anonymity that reflect cultural, legal, and ethical priorities but increasingly converge in seeking balance:

- Europe: The EU's General Data Protection Regulation (GDPR) sets a high bar for privacy, allowing pseudonymization (limiting identification without full anonymity) but excludes fully anonymous data from its rules. European courts mandate strict judicial oversight for targeted data access in serious crime cases, balancing privacy and policing needs.
- United States: Laws like the California Consumer Privacy Act (CCPA) strengthen privacy rights but do not guarantee complete anonymity. The focus is on transparency, user control, and data security, while law enforcement may access data under legal procedures.
- Brazil and Latin America: Laws like Brazil's LGPD, inspired by GDPR, emphasise purpose limitation, transparency, and accountability, while allowing legal data transfer frameworks. Many Latin American countries regulate data flows strictly, ensuring cross-border privacy protections with mechanisms like explicit consent or data adequacy decisions.

- Asia Pacific and Middle East: Regions are rapidly updating data protection laws, inspired by international standards but adapted to local contexts, aiming to secure privacy while enabling lawful data use. For example, South Africa's POPIA and reforms in Australia and South Korea embed principles of responsible processing with accountability.
- UK: The 2025 Online Safety Act tries to harmonise user protection and platform responsibility by enforcing content moderation alongside strong encryption safeguards and strict legal oversight for data access, as a middle way between perfect privacy and public safety.

The Cost of Online Fraud and Scams

One group that benefits from the privacy and anonymity afforded by current technologies are fraudsters. As of 2025, global online fraud and scam losses are estimated to exceed $1 trillion annually, representing a significant and growing share of the broader $10.5 trillion total global cybercrime cost forecasted for the year[2].

Breakdown of Global Fraud and Scam Losses

- The Global Anti-Scam Alliance (GASA) reported that scammers stole $1.03 trillion worldwide over the past 12 months, with only 4% of victims recovering all their losses[3].
- The Cybercrime 2025 report by CompTIA projects total global cybercrime losses—including online fraud, scams, ransomware, phishing, and data breaches—to reach $10.5 trillion annually by 2025, reflecting both direct theft and related costs like business disruption and reputation damage[4].
- Data from Scam Statistics 2025 shows that scams involving digital channels (social media, websites, apps, and blockchain) dominate global reports. The U.S., U.K., India, Nigeria, and Brazil rank among the most affected nations[5].

[2] https://explodingtopics.com/blog/number-of-scams

[3] https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai

[4] https://deepstrike.io/blog/cybercrime-statistics-2025

[5] https://sqmagazine.co.uk/scam-statistics/

These figures highlight how online scams have evolved into a trillion-dollar criminal economy, driven by AI-enhanced deception (such as deepfake and voice clone scams), social media fraud, and cryptocurrency investment schemes. The $1 trillion in direct scam losses represents roughly 10% of the global cybercrime economy, underscoring the growing sophistication and automation of digital fraud networks.

Online Harms to Children

Children are especially vulnerable in environments where anonymity protects predators and harmful actors. Perfect anonymity allows online predators to operate with impunity, grooming and exploiting minors without any trace. Perfect privacy hinders parents, educators, and platform providers from monitoring or intervening when children encounter bullying, misinformation, or harmful content. As digital spaces expand, safeguarding children becomes increasingly complex without careful privacy-accountability balances.

Research is available that illustrates the degree of risk to children from perfect privacy and perfect anonymity. For example, Childlight[6], a child safety research institute, published a report in November 2023[7] that measured the prevalence of offending, risk behaviours and attitudes amongst a weighted sample of men over 18 years of age: 1,945 Australians, 1,473 from the UK and 1,506 from the US.

The findings included the following:

- Men in the survey who reported engaging in at least one online offending behaviour against children in all three countries were at increased risk of reporting they would also seek sexual contact with a child between the ages of 10 to 12 years old if they could be certain that no one would find out, compared to men who reported no online child sexual offending behaviours.
- Over 1 in 20 surveyed men from Australia, the UK and the USA said they were ‘definitely’ or ‘highly likely’ to have sexual contact with a child between the ages of 10 to 14 years old if they thought no one would find out.

[6] https://www.childlight.org/

[7] https://www.childlight.org/searchlight/the-nature-of-online-offending-against-children-population-based-data-from-australia-uk-and-the-usa

- A significant proportion (13-16% of surveyed men across the three nations) said they would consider having sexual contact with a child if they knew no one would find out.

Whilst several factors contribute towards the risk of being caught, perfect privacy and anonymity clearly play a significant role.

Is this just a theoretical risk? Many of us underestimate the current scale of online child sexual abuse and exploitation (CSAE). Estimates by Childlight[8] suggest that there are 300 million victims per annum (see Into the Light report 2024[9], page 3), that's nearly 14% of children in the world. And research by Protect Children[10] has highlighted the widespread use of messaging platforms by paedophiles to share CSAM (see Tech Platforms Used by Online Child Sexual Abuse Offenders[11], page 11).

The Internet Watch Foundation has noted the use of end-to-end encryption by criminals seeking to blackmail children who have shared explicit images, a practice known as "sextortion." Offenders typically target children on mainstream platforms before getting them to move on to encrypted messaging services to continue the extortion. The practice is growing in significance, and the impact can be devastating, sometimes resulting in suicide[12].

Conclusions and Recommendations

Privacy and anonymity are not absolutes but require calibrated limits that protect both individual freedoms and societal safety. International legal frameworks are increasingly reflecting this balance, which is crucial for safeguarding children and combating crime without sacrificing core privacy values.

[8] https://www.childlight.org/

[9] https://www.childlight.org/uploads/publications/into-the-light.pdf

[10] https://www.suojellaanlapsia.fi/en

[11] https://bd9606b6-40f8-4128-b03a-9282bdcfff0f.usrfiles.com/ugd/bd9606_0d8ae7365a8f4bfc977d8e7aeb2a1e1a.pdf

[12] https://www.bbc.co.uk/news/articles/czrpedexleno

The above position has not yet been reflected in technology changes, where the trend continues towards ever stronger privacy protections, and where tools continue to be developed that offer anonymity. For example, changes to Internet protocols are continuing to favour privacy protections, and applications are using ever stronger encryption techniques[13],

To mitigate the corrosive effects of perfect privacy and anonymity, global trends suggest layered solutions:

1. Allow pseudonymity and selective disclosure to maintain user privacy without eliminating accountability.
2. Enforce judicial oversight and transparency for any law enforcement access to private data.
3. Mandate social media and messaging platforms to monitor and act on illegal or harmful content without compromising encryption and in a privacy-preserving manner. For example, it is straightforward to prevent the sharing of known CSAM by using client-side scanning[14], taking advantage of hash matching techniques.
4. Promote international data governance cooperation to handle cross-border privacy and crime issues effectively.
5. Increase digital literacy initiatives aimed at children, parents, and educators to recognise and address online risks, ideally complemented by more effective and more accessible parental controls[15].

Dialogue is needed between all parties. Whilst privacy is important, those in favour of perfect privacy and anonymity need to understand that there are potentially significant costs if this quest succeeds, many of which are likely to be borne by vulnerable groups.

[13] https://arstechnica.com/security/2025/10/why-signals-post-quantum-makeover-is-an-amazing-engineering-achievement/

[14] https://419.consulting/client-side-scanning

[15] https://419.consulting/parental-controls

