CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

SUBMISSION:

The House of Representatives Select Committee on Social Media and Online Safety's Inquiry into Social Media and Online Safety

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: Inquiry into Social Media and Online Safety

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) submission to the House of Representatives Select Committee on Social Media and Online Safety for this inquiry. This inquiry is particularly timely given the ever-increasing role social media and other online platforms play in the lives of all Australians. Online safety must be a key consideration as Australia continues to evolve as a digital economy and is essential for ensuring that our nation not only remains a safe and secure digital nation, but also that the most vulnerable members of our community are protected.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

We look forward to answering any queries about this submission and welcome the opportunity to participate in future discussions regarding this very important topic.

Yours Sincerely,

[redacted]

Rachael Falk
CEO, Cyber Security Cooperative Research Centre
ceo@cybersecuritycrc.org.au

Executive Summary

The Cyber Security Cooperative Research Centre (CSCRC) welcomes the opportunity to provide this submission to the House of Representatives Select Committee on Social Media and Online Safety. Such an inquiry is timely and pertinent given the widespread impacts of social media and digital technologies on our world, both offline and online.

We live in a digital and interconnected world. Increasingly, our daily activities, transactions and communications are conducted online, via social media and online technology platforms. While providing access to vast troves of information, real-time connectivity and facilitating a diverse online public sphere, social media platforms and their applications can also have negative impacts on societies and individuals. Fuelling cyber bullying and terrorist or violent extremist ideology, providing platforms for the free circulation of child exploitation material (CEM), as well as enabling cyber crime through technological developments such as encryption, these applications and their use or misuse have the potential to erode democratic processes and social norms. In particular, online harms and their negative impacts on the wellbeing and privacy of citizens around the world, including Australians, are growing.

Too often, these online societal and individual harms are occurring on popular social media platforms, created and managed by the world's most prominent technology companies. The interconnected nature of our digital world means that impacts are ubiquitous and global, including among the Australian community. In October 2021, damaging allegations about Facebook's focus on profits at the expense of people came to light, with testimony in U.S. Congress by whistle blower Frances Haugen.[1] Presenting evidence that Facebook was aware that its Instagram platform algorithms were designed to lead young users to eating disorder-related content, known to be damaging to the mental health of teenagers, the testimony was heralded as a potential 'big tobacco' moment for social media giants.[2]

Facebook also faced scrutiny for its alleged role in the spread of misinformation and the undermining of democracy. Haugen's testimony outlined how the technology giant knowingly focused on maximising user engagement and growth through continued reliance on its proprietary algorithms, even though doing so was known to stoke political tensions.[3] This is not the first time large social media companies have faced criticism concerning their practices and impacts on political processes. In August, the U.S. troop withdrawal in Afghanistan led social media giants like Twitter and Facebook to wrestle publicly with how to effectively moderate official Afghan government accounts, given the Taliban has long relied on digital platforms as potent vehicles to spread its ideology. The incident raised moral and ethical questions for large social media platforms

[1] Facebook whistleblower testimony should prompt new oversight – Schiff | Facebook | The Guardian
[2] Facebook whistleblower testimony should prompt new oversight – Schiff | Facebook | The Guardian
[3] Frances Haugen says Facebook's algorithms are dangerous. Here's why. | MIT Technology Review

about their societal obligations to curtail social media activity which may seed unverified narratives or perpetuate falsehoods. This follows the 2016 allegations about Facebook's impact on the 2016 U.S. Presidential election, given its unmatched ability to propagate political information across the internet, largely unchecked.[4]

Also of concern is the growth of online radicalism and extremism, often fuelled by social media platforms. The online world plays a key role in fostering connections, influencing views via algorithms and enforcing extremist ideologies through the proliferation of social media and encrypted communication platforms. The CSCRC contends that social media companies have moral, social and legal obligations to disrupt and deter extremism and radicalism online, starting with greater transparency about the algorithms they deploy, reflecting growing global consternation about the manipulative power of algorithms to create extremist echo chambers.[5] [6]

Accordingly, governments worldwide are seeking to rein in the power of social media platform providers through laws that regulate social media companies and mitigate online harms. The CSCRC supports the Federal Government for its position, not only with this important inquiry, but with the passage of two significant pieces of legislation in 2021 which bolster Australia's powers to boost online safety and prevent serious cyber-enabled crime: the *Online Safety Act 2021* and the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021* (SLAID). Further, the December 2021 introduction of the *Social Media (Anti-Trolling) Bill* will bolster legal responses to online cyber bullying.

This submission will address the following key issues:

(a) the range of online harms that may be faced by Australians on social media and other online platforms, including harmful content or harmful conduct;

The CSCRC supports the Australian Government's endeavour to gain a better understanding of the online harms that Australians may face on social media and other platforms. The concern for the rights and interests of all Australians in accordance with domestic and international human rights principles is commendable and resonates with Australia's long tradition as a liberal democracy.

However, this is no small task. The online and offline worlds are inextricably linked. This has only increased under the working from home (WFH) conditions induced by the COVID-19 pandemic, with many citizens increasingly living life online. There have been numerous negative societal impacts, including the growth of online abuse and harms directed at Australians. The Australian Office of the

[4] What Facebook Did to American Democracy - The Atlantic
[5] You and the Algorithm: It Takes Two to Tango | by Nick Clegg | Medium
[6] Facebook Is a Doomsday Machine - The Atlantic

eSafety Commissioner highlighted a 30 per cent increase in reports of child cyber bullying in 2020 and 40 per cent for adults, underscoring the need for more to be done to prevent such activity.[7]

One significant result of Australians spending more time online is the vast proliferation of digital personal data being generated. Australians, while avid users of social media platforms and applications, are hungry for accessible information about privacy and the protection of their personal information.[8] The Office of the Information Commissioner (OAIC's) 2020 *Australian Community Attitudes to Privacy* survey found Australians support more easily readable privacy policies on internet websites, given their current presentation is an impediment – only one in five read and are able to understand these policies.[9] At times this lack of awareness has proved far more serious, amounting to allegations that Australian consumers are not just unaware, but have been misled by technology companies about the collection of their personal data. In July 2020, the Australian Competition and Consumer Commission (ACCC) commenced proceedings against Google on these grounds, "alleging Google misled Australian consumers to obtain their consent to expand the scope of personal information that Google could collect and combine about consumers' internet activity, for use by Google, including for targeted advertising".[10] Hence, there is a need for industry to enhance the accessibility of privacy and consent notices to Australian social media platform users and ensure the wording is fit-for-purpose for the digital age, to build user confidence and awareness of how information is being collected and who it is being shared with. Furthermore, it is common sense that such notices should be regularly updated and conveyed in clear, easily understood language, with details of how the information is used and disclosed. The ACCC's *2019 Digital Platforms Inquiry* report found that users give initial sign-up consent when they begin using digital platforms, however this does not account for changes which may take place after sign-up.[11] The CSCRC also submits that it would also be useful to consumers to know the jurisdiction within which their data is being held.

The strengthening of consent requirements to increase the transparency of information collection and reduce the bargaining power imbalance between consumers and relevant entities can also be achieved through other mechanisms. In particular, the CSCRC supports the principle that: "valid consent should require a clear affirmative action that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent). This means that any settings for data practices relying on consent must be pre-selected to 'off' and that different purposes of data collection, use or disclosure must not be bundled".[12] The CSCRC strongly supports the inclusion of 'off' default settings for information that is not required for the provision of

[7] Australia's eSafety Commissioner targets abuse online as Covid-19 supercharges cyberbullying | The Strategist (aspistrategist.org.au)
[8] Australian Community Attitudes to Privacy Survey 2020 (oaic.gov.au), pp 8
[9] Australian Community Attitudes to Privacy Survey 2020 (oaic.gov.au), pp 8
[10] Correction: ACCC alleges Google misled consumers about expanded use of personal data | ACCC
[11] Digital platforms inquiry - final report.pdf (accc.gov.au), pp 395
[12] Digital platforms inquiry - final report.pdf (accc.gov.au), pp 35

products or services by social media platforms because changing such settings is illustrative of meaningful consent.

Further, although the provisions and frameworks established under the *Privacy Act 1988 (Cth)* (the Act) provide specific safeguards for the privacy of individuals, these protections are not absolute. The rapid evolution of technology, namely the interconnectedness brought by the internet, has impacted the world profoundly since the Act was established. This has had serious ramifications for the privacy of individuals and protection of their personal data, which remains vulnerable to data breaches which can have harmful impacts on Australians.

To further address online harms resulting from a potential data breach, a new Commonwealth tort dealing specifically with cyber harms as a result of a digital privacy breach would help provide clarity in what remains a grey area, because in Australia there is no charter of rights or specific constitutional or tortious right to privacy. While the Act does provide limited protections, the law and its interpretation are murky despite the fact cyber harms resulting from data breaches are real, tangible and damaging. Given the rapid proliferation of personal information being shared via digital means, it is a logical inference such harms could also become increasingly common. Therefore, the law needs to be sufficiently prepared. Such a tort would provide a clear mechanism through which individuals could seek to protect their privacy, which extends beyond the protections offered in the Act.

(b) evidence of:
(ii) the extent to which algorithms used by social media platforms permit, increase or reduce online harms to Australians;

Australian consumers and internet users should be made aware that online content is *never neutral*. Rather, the content and information which Australians consume via social media platforms is curated according to the business model needs of social media companies, accustomed to maximising growth and maintaining access to users data as the primary business driver. This curation is largely achieved by algorithms, computer codes which are readily deployed by many of the world's largest social media platforms to align with a user's interests. Incorporating machine learning and artificial intelligence technologies, algorithms may risk replicating and amplifying pervasive human biases, including racial and gender biases, and therefore require further ethical considerations.

In August 2021 the CSCRC made a submission to the Parliamentary Joint Committee on Law Enforcement (PJCLE) on *Law Enforcement Capabilities in Relation to Child Exploitation*. The submission highlighted that the advent of the internet has been a boon for child sexual offending and the production and distribution of child abuse material (CAM). It also underscored that efforts to counter these offenses lie not only with law enforcement agencies, but that this is a shared responsibility and there is a clear role for technology providers to help law enforcement combat CAM through the monitoring, removal and reporting of such content, as well as through technological developments. This action is vital, given the significant amount of CAM detected on Facebook. For example, in 2020 the US National Centre for Missing and Exploited Children (NCMEC) reported Facebook was responsible for 94 per cent of the 69 million child sex abuse images reported by US technology companies.[13]

To an extent, such support is rendered by digital platform providers.[14] However, more work can be done, particularly as it comes to greater transparency concerning the creation and usage of algorithms and resulting innovative technologies deployed by large social media companies to combat online CAM. For example, Microsoft's PhotoDNA is used globally to detect, disrupt, and report millions of child sexual exploitation images. Likewise, Google's Content Safety API has improved the ability of NGOs and other tech companies to review CAM and Facebook's open-source photo- and video-matching technology employs hash-sharing systems to communicate, assisting in the detection of duplicated CAM. In the US, Apple recently launched *neuralMatch*, which scans images from Apple devices before they are uploaded to iCloud, and also has plans to scan users' encrypted messages for CAM.[15]

Despite these positive technological developments, the CSCRC notes there is little transparency around the design of these technologies and the algorithms they deploy which shape them. Facebook's submission to the PJCLE's inquiry noted its free, open source technology had been made available to industry, developers and NGOs, as well as the Australian Federal Police (AFP), which deployed it after reviewing the algorithms.[16] Further, Facebook highlighted the ongoing development of additional tools and activities to mitigate inappropriate interactions between minors and adults, noting Australia is one of the first jurisdictions in the world to leverage these algorithms. Google's submission to the PJCLE's inquiry highlighted its free Content Safety API, created in 2018, which leverages classifiers (algorithms) to help Google sift through billions of images to prioritise those which may contain abusive material before they are flagged for human review.[17]

These developments are commendable. However, the CSCRC urges that more clarity and transparency must be provided concerning their technical development, given their utilisation of artificial intelligence and machine learning technologies, which are themselves not un-biased technologies. The potential establishment of future accountability measures, including legal, will help ensure algorithms are non-biased, developed ethically, and will not have negative and

[13] Facebook Rolls Out New Tools To Stop 'Non-Malicious' Child Exploitation (forbes.com)
[14] Google, Facebook and Microsoft back plan to combat child sexual abuse (cnbc.com)
[15] Apple to scan U.S. iPhones for images of child sexual abuse - ABC News (go.com)
[16] Submissions – Parliament of Australia (aph.gov.au), Facebook, pp 3
[17] Submissions – Parliament of Australia (aph.gov.au), Google, pp 4

unforeseen impacts on society. In 2020, the Australian Human Rights Commission's (AHRC) *Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias* paper warned unfair outcomes arising from algorithmic bias could result in unlawful discrimination under Australian law and advised businesses to be "proactive in identifying the human rights risks in how they use AI".[18] Further, the development of these algorithmic tools must coincide with ongoing consultation with relevant law enforcement agencies and civil society organisations to ensure they are designed in accordance with legal checks and balances, especially concerning privacy, not as an afterthought.

(c) the effectiveness, take-up and impact of industry measures, including safety features, controls, protections and settings, to keep Australians, particularly children, safe online;

&

(e) the transparency and accountability required of social media platforms and online technology companies regarding online harms experienced by their Australians users;

The CSCRC notes that social media companies are taking significant steps to bolster the security, protections and transparency of their online services and their impacts on Australians to keep users safe online. It is commendable to note this is also happening in lockstep with government. On the second anniversary of the Christchurch Call in May 2021, more than 50 government and technology companies banded together to commit to collaborative approaches to improving collective responses to terrorist and violent extremist threats.[19] Participants including companies such as Facebook, Amazon and Twitter, pledged to undertake more research investigating the role social media algorithms play in online radicalisation. They also pledged to boost transparency concerning efforts to minimise terrorist online content by establishing a world-leading global Voluntary Transparency Reporting Framework. Such approaches are indicative of a shared social responsibility model in action. Further, Google was involved in the design of the eSafety Commissioner's *Safety by Design Principles* and has publicly vowed to uphold these.[20]

These steps are admirable. But more needs to be done by industry, given the gravity of the potential societal risks involved. In particular, the CSCRC has previously highlighted the challenge which encrypted platforms used by technology companies pose to law enforcement agencies as it comes to mitigating illicit online activity, including the spread of terrorist ideology.[21] Encryption is the conversion of information or data into unintelligible code, which prevents unauthorised access.

[18] Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias (2020) | Australian Human Rights Commission, pp 8
[19] Christchurch call further bolsters online safety (homeaffairs.gov.au)
[20] Submissions – Parliament of Australia (aph.gov.au), Google submission, pp 1
[21] CSCRC - SLAID submission.pdf (cybersecuritycrc.org.au), pp 12, 13

While encryption plays a key role in keeping personal and valuable information protected, it is also widely used by criminals to cloak their illicit activities, making it difficult for law enforcement to lawfully intercept and read messages criminals send to each other.

End-to-end encryption provides a form of communication protection that prevents third parties – including internet service providers, app hosts and law enforcement – from accessing data transferred from one system or device to another. This means data is encrypted on one system or device and only the recipient (who receives the communication) can decrypt it.

End-to-end encryption software built into instant messaging apps means a third-party intercepting the messages cannot read them, as they will be indecipherable. These services operate 'over the top' of traditional telephony networks, which means it is impossible to know when they are even being used. Examples of well-known encrypted instant messaging apps include Telegram and WhatsApp. Facebook Messenger is not currently encrypted by default, but this feature can be enabled. There is also a high risk that if, as planned, Facebook adopts end-to-end encryption across its services, it will act as a new forum through which extremists can conceal their communications and activities.

Such concerns have been raised by Department of Home Affairs Secretary, Mike Pezzullo, who told a Senate Estimates hearing in 2020 that: "We are particularly concerned about Facebook's plans to go to end-to-end encryption of their entire platform to create, in effect, the world's biggest dark web".[22] Facebook has acknowledged the challenges that encryption poses to law enforcement, while affirming its commitment to moving towards end-to-end encryption on its Messenger platform.[23] Likewise, Google has affirmed its ongoing commitment to deploying end-to-end encryption for private conversations between Android Messages users, noting the company has at its disposal 'behavioural information and meta-data signals' which can be utilised to mitigate CAM in encrypted environments.[24] However, it is worth noting that metadata itself is inherently opaque. Although Google notes more work needs to be done to ensure these tools are deployed lawfully, there is further scope for this to be done in consultation and collaboration with government, to build transparency and accountability measures into the process. Such consultation should be broad and include regular and ongoing engagement with relevant Australian Government entities, including law enforcement, to ensure outcomes are effective and designed with broader societal considerations in mind.

Taking a proactive approach to technical solutions is advisable as law enforcement agencies continue to grapple with the challenges of encryption. Criminals are known to be early adopters of new technologies that help evade detection. On this front, it has been predicted by some that the

[22] Hansard - Committee 19/10/2020 Parliament of Australia (aph.gov.au)
[23] Submissions – Parliament of Australia (aph.gov.au), Facebook, pp 16
[24] Submissions – Parliament of Australia (aph.gov.au), Google, pp 2, 3

'decentralised web' will become a new way for criminals to communicate and evade authorities.[25] This would in effect mean criminals would be able to store data and communicate via their own servers, mitigating the effect(s) of content takedowns by creating an independent, decentralised storage network outside the grasp of service providers and law enforcement.[26] These activities were on display in the June 2021 revelation of Operation Ironside, an AFP-led operation whereby criminals leveraged an exclusive encrypted communications platform to perpetrate their crimes.[27] There is also a likelihood criminal groups could move to encrypted platforms produced outside the West, in less stringently governed states.[28] To this end, it is also likely such groups will move to build their own encrypted platforms or purchase already developed platforms from the dark web.[29]

(f) the collection and use of relevant data by industry in a safe, private and secure manner;

The safe, private and secure collection and storage of data by industry is a pressing concern, given the widespread proliferation of data and urgent need to ensure cyber secure best practices. A recent survey by the OAIC measuring Australian attitudes to privacy found that one of the biggest privacy risks identified by Australians are digital services, including social media sites.[30] Globally, cyber security remains a foremost consideration when it comes to the protection of valuable data, given its vulnerability to data breaches and leaks. The Cambridge Analytica data harvesting scandal disclosed in 2018 underscores the sobering potential impacts of data breaches on citizens and consumers.[31] In this instance, Facebook was said to have seriously failed to secure users' personal data, when it was revealed that 50 million user profiles had been compiled in a massive data breach in efforts to sway American voters. Further, malicious cyber actors continue to hone tactics, state-of-the-art methodologies and strategies to access vast troves of personal data for nefarious purposes and financial gain, including illicit trade on the dark web. In July 2021 it was revealed the personal data of more than 90 per cent of LinkedIn's users had been scraped from LinkedIn's website and posted for sale online by hackers.[32] While LinkedIn claimed the episode was not an instance of a cyber attack but rather a data scrape, the posting of the vast trove of data on websites frequented by hackers could leave affected users vulnerable to malicious cyber activity such as phishing scams along with having their personal information circulate on the dark web.

Given these ongoing risks, the CSCRC submits there needs to be more transparency provided by the technology sector about how data on consumers is accessed, collected and stored. At all times, it is

[25] Commonwealth Director of Public Prosecutions v CCQ [2021] QCA 4 (22 January 2021) (austlii.edu.au), p 23
[26] Ibid, 47 pp 23
[27] AFP-led Operation Ironside smashes organised crime | Australian Federal Police
[28] Commonwealth Director of Public Prosecutions v CCQ [2021] QCA 4 (22 January 2021) (austlii.edu.au), 47 pp 37
[29] Ibid 47 pp 37
[30] Australian Community Attitudes to Privacy Survey 2020 (oaic.gov.au), pp 6
[31] ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information | ICO
[32] LinkedIn data theft exposes personal information of 700 million people | Fortune

essential innovation gains remain balanced by cyber security and privacy considerations. This could entail greater accountability measures and mechanisms enforced by government, which social media companies must abide by. This should include greater transparency for consumers about how their data is collected and utilised. Further, simple advice in accessible language could be provided to consumers if and when their data is compromised about *what* to do to better protect information and *how* to do it, including changing passwords; reassessing personal information available on social media; and advice urging users to be cautious when connecting with others on social media platforms. In addition, social media companies need to provide greater visibility as to how users' data is stored, and the cyber security measures and protections deployed to ensure the ongoing safety of that data.

To that end, government might consider global best practice approaches for industry, such as those like the European Union's General Data Protection Regulation (GDPR). The GDPR regime offers a progressive approach to the management of data and privacy risks of citizen data, taking a human-centric approach, and it has tangible impacts on social media companies using large amounts of data and collecting personal data on EU residents. The GDPR is fundamentally built around the premise of 'privacy by design' which seeks the protection of individual privacy and limits the untrammelled collection of data by organisations, creating a strong legal basis for ethical and transparent data collection and usage. Adoption of similar measures would have the additional benefit of fostering international regulatory harmonisation.

(g) actions being pursued by the Government to keep Australians safe online; and

Australia has been leading the world in online regulatory reforms which aim to keep Australians safe online, and which are setting the global standard for best practice. There are three key reforms in this regard. First, the August 2021 passage in Australian Parliament of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021* (SLAID) is notable. The law equips the AFP and the Australian Criminal Intelligence Commission (ACIC) with greater legislative powers to conduct online investigations on key threats including terrorism and violent extremism. The evolving online threat environment and surging use of anonymising and encrypted technologies have afforded criminals unprecedented ways to facilitate their crimes. Australia is the first jurisdiction in the world to have such a suite of powers available to law enforcement and intelligence agencies, with strong safeguards and oversight included to ensure these powers are proportionate, used as intended and in accordance with the law. This additional rigour also upholds the privacy and civil liberties of all Australians to ensure they are not adversely affected by the use of these legitimate and necessary powers.

In addition, in June 2021 the *Online Safety Act* was enacted which significantly enhances the powers and remit of Australia's Office of the eSafety Commissioner to protect Australians from serious online harms. The legislation, effective from 23 January 2022, reflects the Australian Government's sober consideration of the rapid pace of technological change, the prevalence of social media in everyday lives, and the unfortunate escalation of cyber abuse and cyberbullying. Significant changes to the updated legislation include a cyber abuse scheme which permits the removal of abusive material if determined to have been undertaken with the intent to cause serious harm. For children, a broadened cyberbullying program has been developed which will equip the eSafety Commissioner with greater powers to prevent further bullying and a scheme has been devised targeting online takedowns of CAM and terrorism-related content.

Significantly, the new Act sets the bar higher for technology companies to provide assurances concerning the safety of their products and services, more transparency concerning their procedures and policies and the future design of industry codes to assist industry in navigating the new regime and their obligations. The latter is to be undertaken together with industry, underscoring that Australia's technology and social media companies have a vital role to play in supporting the work undertaken by law enforcement and intelligence agencies to safeguard Australia online.

Lastly, the December 2021 introduction of the *Social Media (Anti-Trolling) Bill* in Australian Parliament will dovetail with the boosted online powers of the Office of the eSafety Commissioner. The proposed powers would compel social media companies to reveal anonymous trolls who may then be subject to defamation liability for defamatory comments.

The CSCRC submits that an absolute right to privacy can never exist and there must always be exceptions, especially when it comes to benefitting all of society. This is a principle recognised in the International Convention of Civil and Political Rights, which makes explicit exceptions where privacy can be overridden, including for the protection of national security, public order, or of public health and morals.[33] The CSCRC contends that while privacy is valuable it must have limitations and these limitations must correlate with the social contract all members of the community enter into, upon which modern democracies like Australia are built. Social contract theory holds that for society to function properly individuals must give up certain rights. This is a concept that can no longer simply be applied to the physical world – in 2021, it must also incorporate unacceptable behaviour that occurs in the digital domain.

[33] OHCHR | International Covenant on Civil and Political Rights