SafeToNet submission to the Australian Government's CCTIES

**Australian Government Call for Submissions: Cyber and Critical Technology International Engagement Strategy (CCTIES)**

Please ensure each submission includes:
**Name and contact details of the individual or body making the submission**

Richard Pursey CEO SafeToNet
rpursey@safetonet.com
c/o SafeToNet Ltd
Floor 6
Imperial House
8 Keen Street
London
WC2B 4AS

**Overview of the author**
Richard Pursey was a seasoned entrepreneur in both the services and software sectors, before starting SafeToNet in 2013.

In 1988 he co-founded Logical Networks and in 1992 he became General Manager of Simmons Magee, a £50 million IT distribution company. He launched a PC-based disaster recovery service and led an MBO in 1993.

Richard has held various board level positions including NED for an NHS Primary Care Trust (Berkshire West) where he learned about mental health issues and in particular the societal problems surrounding child abuse.

**Submissions must consider at least one of the following questions:**

**What should Australia's key international cyber and critical technology objectives be? What are the values and principles Australia should promote regarding cyberspace and critical technology?**

The key international cyber and critical technologies for Australia should be to help make accessing the internet safe for all, especially our most vulnerable members of society – children and vulnerable young adults. Lethal cyberbullying, grooming, sextortion and radicalisation are caused by a technological free for all when it comes to accessing children online. The internet, and the World Wide Web that sits on top of it, provides our children with access to the world, but is also provides the world with access to our children.

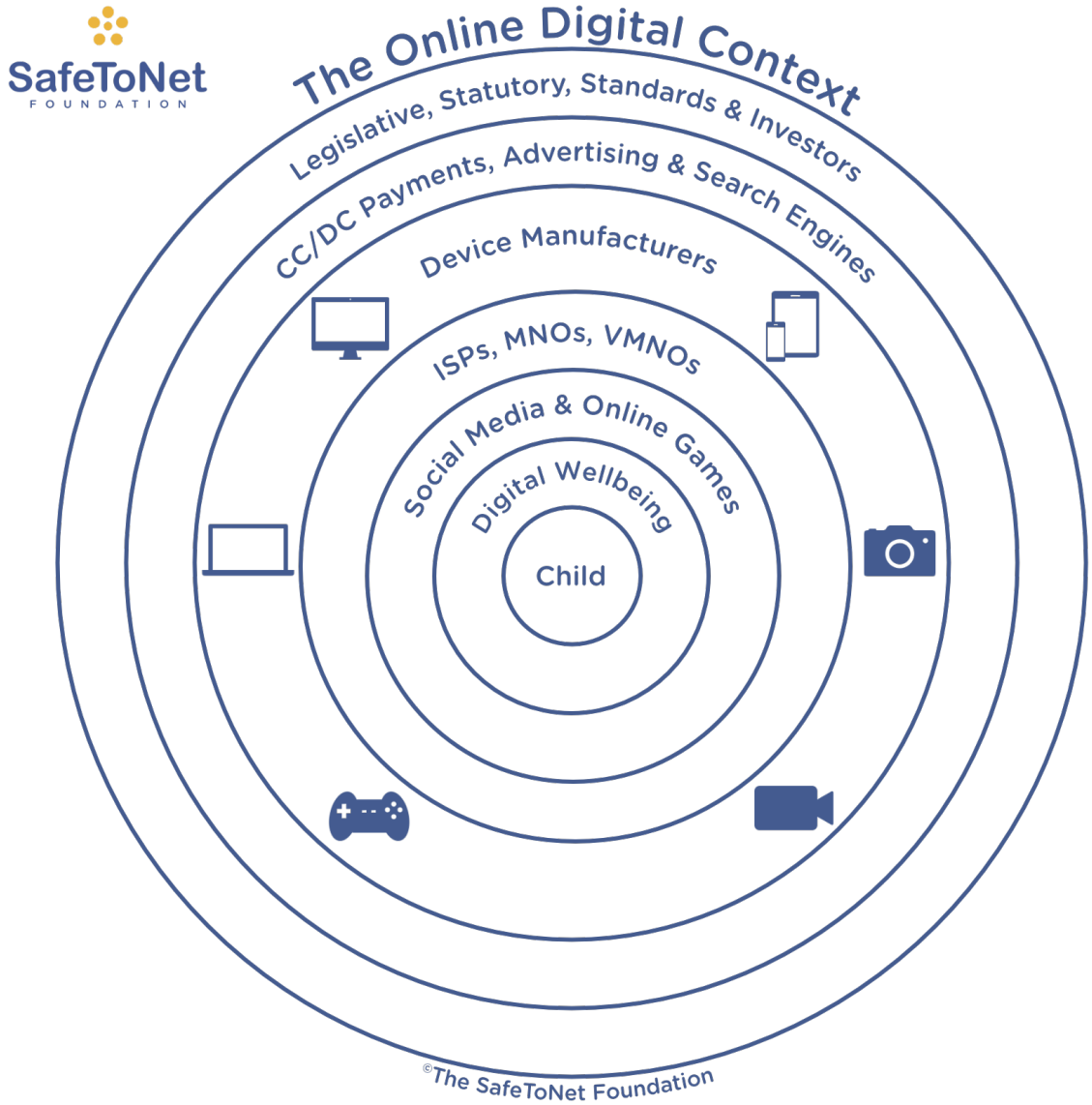
In the words of the UK's former Chief Superintendent of London's Metropolitan Police Dal Babu: *"If you were a paedophile and you were looking to invent a system for abusing children, identifying them, grooming them, being able to meet them where your safety was guaranteed to carry out acts for your sexual gratification, you'd invent the internet."*[1]

As things currently stand, the Western social media companies are mostly based on the West coast of the USA and therefore fall under the legal jurisdictions of the Federal US and Californian State laws. Section 230 of the Communications Decency Act provides these companies with immunity from liability for content posted on their platforms and relies on self-regulation. However the circulations of billions of child sex abuse images online shows this simply isn't working.

[1] Dal Babu OBE, former Chief Superintendent Met Police, SafeToNet Foundation podcast, 2019.

Until this immunity from liability changes, then the international community needs to work together with technology and other laws to change culture and to protect children's online experience. Australia has made a great start by appointing an eSafety Commissioner (Julie Inman-Grant) who is promoting "Safety by Design" for tech companies, and by passing laws such as Carly's law which is being taken seriously internationally and a version of it, the "Sexual Communication with a Child" Act has been passed in the UK. But more needs to be done.

SafeToNet respectfully suggests that Australia adopts a child centric view of the World Wide Web and underlying internet, and mandates technologies that can be implemented by, and laws that can be followed by, all organisations that provide a social media functionality within their online services. A child-centric Online Digital Context expands the concept of the UK's offline Contextual Safeguarding model to the online, and looks like this:




Tesla were granted no exceptions from car safety laws just because they were a start-up manufacturer. There is no reason at all why online companies should not be mandated to follow child safety laws.

The overriding principle should be to make the World Wide Web, the internet, social media and online games safe spaces for children. Every service or product or technical specification should place child safety at its core, and should answer the question: "What are the consequences for child online safety of this product or service or specification?".

Children have fundamental rights, and to participate online unmolested is one of them.

**How will cyberspace and critical technology shape the international strategic/geopolitical environment out to 2030?**

2030 is an interesting date, partly because it's now just under a decade away but mostly because that's the date by which the UN expects to meet its target Sustainable Development Goals (UN SDGs):
**UN SDG 3** Ensure healthy lives and *promote wellbeing for all at all ages*
**UN SDG 9** Industry, Innovation, Infrastructure: to develop quality, reliable, sustainable and resilient infrastructure to support economic development *and human wellbeing*
**UN SDG 11** Sustainable cities and communities – This should extend to *online communities*
**UN SDG 16** Promote peaceful and inclusive societies… accountable and inclusive institutions at all levels – (*SafeToNet observation: today social media companies are by law not accountable*). **16.1.4** Proportion of population that feel safe walking alone around the area they live (*SafeToNet observation: create safer spaces by implementing Contextual Safeguarding*). **16.2** End abuse, exploitation, trafficking and all forms of violence against and torture of children (*SafeToNet observation: this extends to all forms of violence in the online space*)

New Zealand has led the world with a national economic plan based not on GDP but on *wellbeing*. Many lessons can be learned by all nations from this innovation. GDP will take care of itself if the focus is on the wellbeing of the population first. The UN's Sustainable Development Goals (UN SDGs) provide a framework for all countries to place the focus of their national growth plans on wellbeing. SafeToNet's focus is the wellbeing of children online.

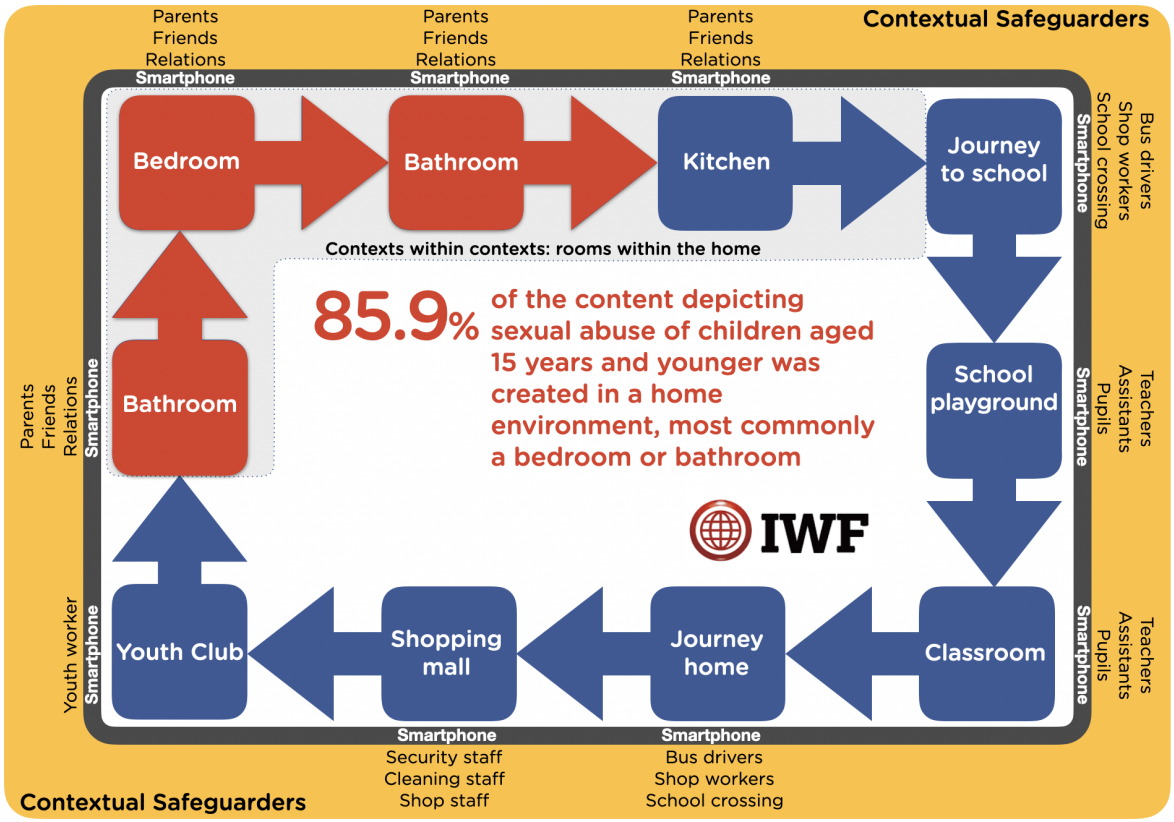
Australia has ratified the 30-year old UN Convention on the Rights of the Child and the more recent Optional Protocols:

- the Involvement of Children in Armed Conflict and
- the Sale of Children, Child Prostitution and Child Pornography.

With this as a solid start, we believe Australia is well positioned to do more in meeting the UN's SDG's by 2030 and to focus on what can be done to end all forms of violence against children from both a legislative and technological perspective. This is an ambitious aim especially given the international and complex nature of the issue, but the frameworks exist for individual Governments to take effective action.

The impact of abuse is on mental wellbeing of children which lasts well into adulthood, also known as Adverse Childhood Experiences (ACEs), which is recognised as a costly burden to the State. In the UK, Statutory guidance of safeguarding children is based on the concept of Contextual Safeguarding, which we respectfully suggest the Australian Government adopts by way of meeting US SDG 16.1.4. However Contextual Safeguarding stops at the online, it offers nothing for safeguarding in the Online Digital Context and won't help Australia resolve children's exposure to online harms.

The online context intrudes into every offline context, as these days where children are, so their smartphone is, so the world can gain access to them:




To address this, we suggest the Australian Government works collaboratively with other Governments and NGOs to put pressure on the US legislature and/or social media companies to take a proactive stance on CSAM[2] and other forms of online harm, to insist that social media companies and companies with social media-like features such as found in online games, have *conditional* immunity from liability for content and messages that pass across their platforms or which are hosted on their platforms. This immunity should only be granted if companies can demonstrate that they comply with child-safety best practices, as proposed in the Federal EARN IT Act currently under consideration in the USA.

The Australian Government can further support the current "Safety by Design" philosophy championed by Australia's eSafety Commissioner Julie Inman-Grant, which includes the 3C's of child online risk, Content, Conduct and Contact, by making safety of children an integral, legally defined component and requirement for creating and distributing social media features, in exactly the same way that other industries have to comply with safety regulations, such as the car industry, the airline industry, the nuclear energy industry. Do not accept the proposition that the internet, or the World Wide Web that sits on top of it, cannot and should not be a safe space for children, or that it will be "broken" if this is tried. Furthermore extend the responsibility through the whole chain from web to child i.e. network operators, broadband providers, handset manufacturers, gaming companies, Ed tech.

By 2030 we believe that it is possible to create safe online spaces for children everywhere, with portable devices that are "Safe out of the Box, which will require the implementation of laws to nudge and shape corporate behaviour as well as on-device technology that is multi-language, real time, platform agnostic, device independent, non-invasive and respectful of the child's right to privacy.

[2] CSAM – Child Sexual Abuse Material

SafeToNet submission to the Australian Government's CCTIES

**What technological developments and applications present the greatest risk and/or opportunities for Australia and the Indo-Pacific? How do we balance these risks and opportunities?**

At SafeToNet we have developed pioneering technology that educated children "in-the-moment" as they use their device. It is a safeguarding assistant that helps children become responsible and safer digital citizens. Its power lies in the smart keyboard that detects risks in real-time. It helps steer children away from trouble by filtering harmful outgoing messages before they can be sent ad before any damage can be done. The smart keyboard provides children with immediate feedback as they type. It recognises signs of low self-esteem and doubt and perhaps most crucially if they are having dark thoughts. It gives messages of support and guidance on how to deal with the issues of living in a digital world.

Parents are a vital part of the solution and research shows that they are concerned about online risks to their children but concede to the benefits of technology. Children are life naïve but social media savvy, parents are life savvy but social media naïve. The feedback from world-leading safeguarding authorities is for the parents and children to have meaningful conversations about being online. So while the advice and guidance we offer children focuses on online behaviours, the advice and guidance we offer parents focuses on social media and the nature of being online and we encourage each to talk to the other.

We are unique in combining a technical solution for children and parents that fully complies with privacy laws and safety by design principles as promoted by Australia's eSafety Commissioner, while permitting children to use the social media platforms they wish to sue and respecting their privacy. We have threaded a path through the technical constraints of both iOS and Android, the legal requirements of the GDPR and other privacy laws such as COPPA, the data handling requirements of the UK's Information Commissioner's Office, the encryption technologies that social media platforms are increasingly using, the obvious requirement to have multiple languages and the UN CRC's rights of the child.

Global, effectively unfettered, access to children by predators represents an unprecedented threat to the most vulnerable in our society, our children, who will have to carry the burden of online harms into their adulthood, damage that is increasingly recognised internationally as Adverse Childhood Experiences (ACE). The Internet Watch Foundation's reports show that the locked family bathroom is the most dangerous place for children to be with a smartphone. How has the world come to this?

The range of risks the social media and online games expose our children to are well documented and summarised by the EU Kids Online project; a child-centric online digital context will address the risks presented by Contact, Conduct and Content:

| | Content<br>Child as a receiver<br>(of mass productions) | Contact<br>Child as participant<br>(adult-initiated activity) | Conduct<br>Child as actor<br>(perpetrator/victim) |
|---|---|---|---|
| **Aggressive** | Violent/gory content | Harassment, stalking | Bullying, hostile peer activity |
| **Sexual** | Pornographic content | "grooming", sexual abuse on meeting strangers | Sexual harassment, "sexting" |
| **Values** | Racist/hateful content | Ideological persuasion | Potentially harmful user-generated content |
| **Commercial** | Advertising, embedded marketing | Personal data exploitation and misuse | Gambling, copyright infringement |

**EU Kids Online classification of Online Risks**

Although these risks are created by weaknesses in current technologies and the legislative environment, they also represent opportunities for technology companies as detailed in the UK's SafetyTech industry, defined and detailed by the UK Government's Department of Culture, Media and Sport (DCMS).

However, technology doesn't operate in a vacuum, and "market forces" can't be relied on when it comes to social media and online games, where monetisation through algorithm-driven clicks and dubious psychological practices, is the number one goal. Government needs to step in to create the legislative and regulatory environment with appropriate and effective sticks and carrots to enable the vibrant but nascent SafetyTech industry to thrive.

The challenge is to create a "techno-legislative" environment that treats children online as a special case, just as they are in the offline world. As children progress through childhood to adulthood, so they have more legal rights and responsibilities: the right to vote, the right to drive, the right to get married, the right to buy fireworks, even the right to own a pet. However currently they seem to bear all responsibility for keeping themselves safe online, which time and again is proving to be ineffective and leads inevitably to victim blaming. Solutions in a child-centric online digital context need to be multi-language, platform agnostic, device independent, real time and respectful of children's rights to privacy.

Balancing the risks vs opportunities cannot be left to "market forces" as is evidenced by the online harms inflicted on children every minute of every day in every country. Technology can be instrumental in creating a phased approach to online digital capability that echoes the offline phased approach that children follow in their journey from childhood to adulthood. But there are no legal incentives for them to do so, only financial incentives for them not to do so. This cannot be left to stand.

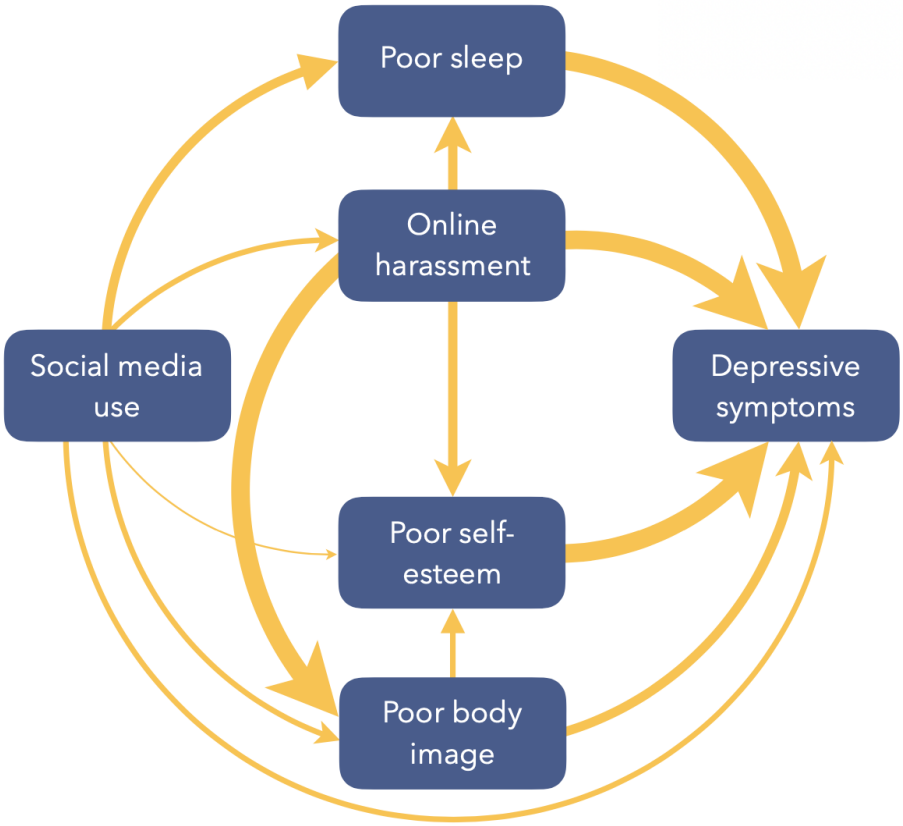
The obvious thing that's common to children from the age of around 9 or 10 is their smartphone. And the one thing that's common to online abuse on all these devices is the keyboard. It's the online *conversations* that lead to abuse, whether cyberbullying or sexploitation. We figured that if the

conversations could be disrupted, we could help reduce the incidents of online harms; but we could do so much more too.

Research published in the UK's Lancet shows that simply using social media could result in depressive symptoms in teenagers, so we endeavoured to also address the mental wellbeing of children.

**How should Australia pursue our cyber and critical technology interests internationally? How can government, industry, civil society and academia cooperate to achieve Australia's international cyber and critical technology interests?**

Online child safeguarding works best when Government, industry, civil society and academia collaborate. Academia can produce rigorous research which can influence Government thinking, legislations and public safety strategies which in turn influence civil society's thinking and attitudes. But even the best academic research is flawed, as demonstrated by the Lancet-published report based on the UK's Millennium Cohort where the key researcher Professor Yvonne Kelly acknowledges inaccuracies in the source data as it relies on self-reporting:

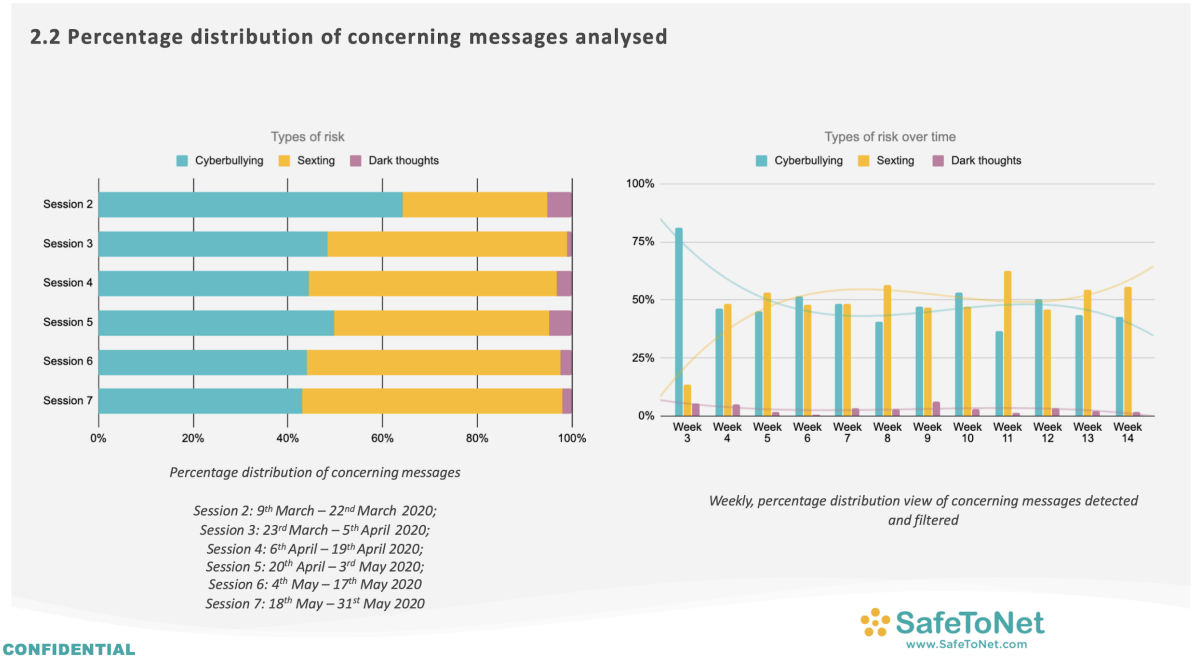



**Social media use and depressive symptoms**

Social Media Use and Adolescent Mental Health: Findings From the UK Millennium Cohort Study published in The Lancet 17.12.2018 shows the relative strength of the different pathways to teens showing depressive symptoms caused by social media usage.

The magnitude of association between social media use and depressive symptoms was larger for girls than for boys. Greater social media use related to online harassment, poor sleep, low self-esteem and poor body image; in turn these related to higher depressive symptom scores.

SafeToNet reports are based on direct interventions of SafeToNet technology on children's smartphone usage. They provide an invaluable insight into the online behaviour of children and how it has changed curing the COVID lockdown for example, in the UK and Germany.




Australia, a key partner in the international "Five Eyes" group of nations, can take a leading role in fostering the development and commercialisation of the indigenous and partner-country "SafetyTech" industry to help bring about a unified technical response to this technical problem. In many ways Australia is leading the way with the appointment of an eSafety Commissioner and passing legislation at a Federal level such as Carly's law. More can be done as a technology-neutral internet favours the abuser.

To do this, we recommend that Australian SafetyTech companies come together and work with the UK's Online SafetyTech Industry Association, OSTIA.

**What policies and frameworks exist in other countries that demonstrate best practice approach to international cyber and technology policy issues?**

From the perspective of SafeToNet we can share the framework and initiative that we currently have ongoing and in place now with the German Government in the accompanying PDF "Government and Business Working Hand in Hand".

Furthermore we are working with the UK Government curing COVID-19 via the SafeToNet Foundation to offer free access to SafeToNet's technology for disadvantaged families to safeguard their children while learning online from home while school access is restricted.

Social media companies have no legal liability for what's posted on their platforms and are fighting proposals to change this. In the meantime we know from organisations across the world such as the IWF, NSPCC, NCMEC and InHope that children globally are being abused in the most degrading ways on these platforms. Yet the UN's Convention on the Rights of the Child states that children have the right to participate, and the right to privacy. Then there's the UN's Sustainable Development goals… So how could this circle be squared?

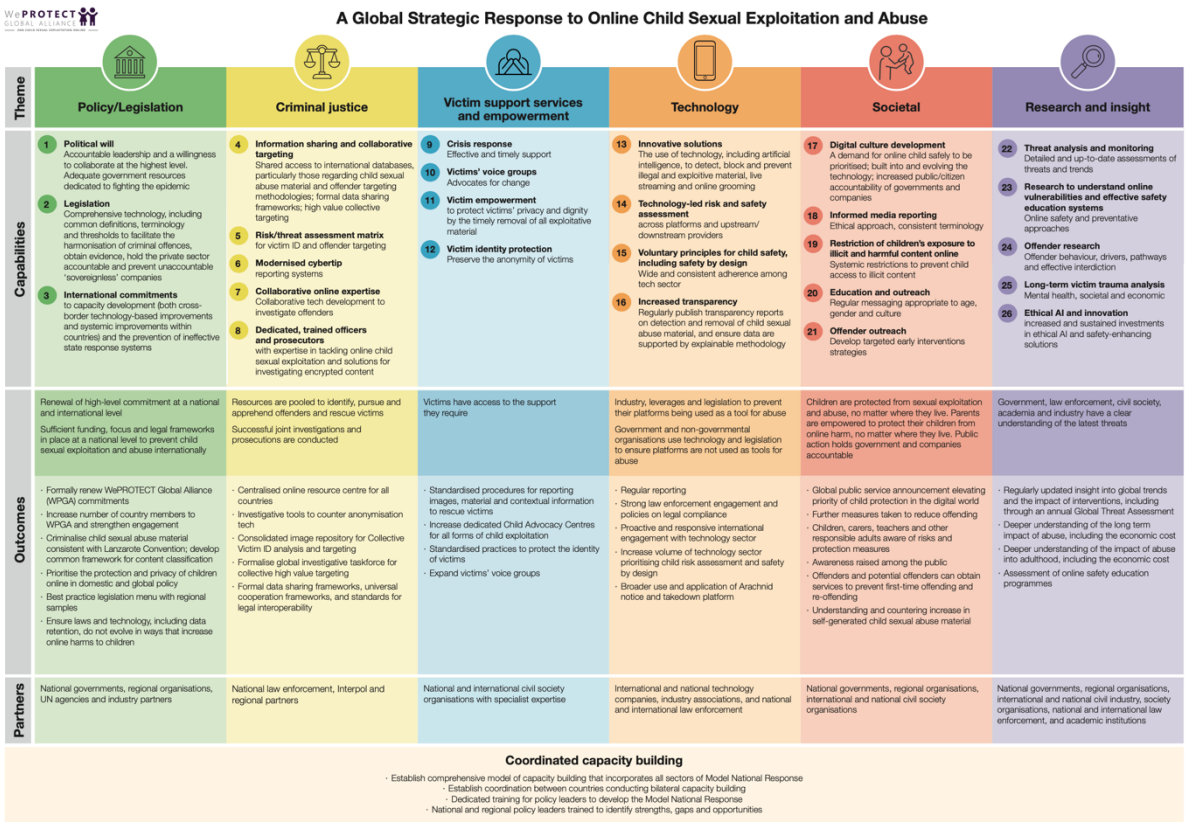
The relevant UN SDG's that relate to online child safeguarding and wellbeing are listed below. This represents a good starting point for national and international time-delimited frameworks, with clearly defined goals in mind.

SafeToNet submission to the Australian Government's CCTIES

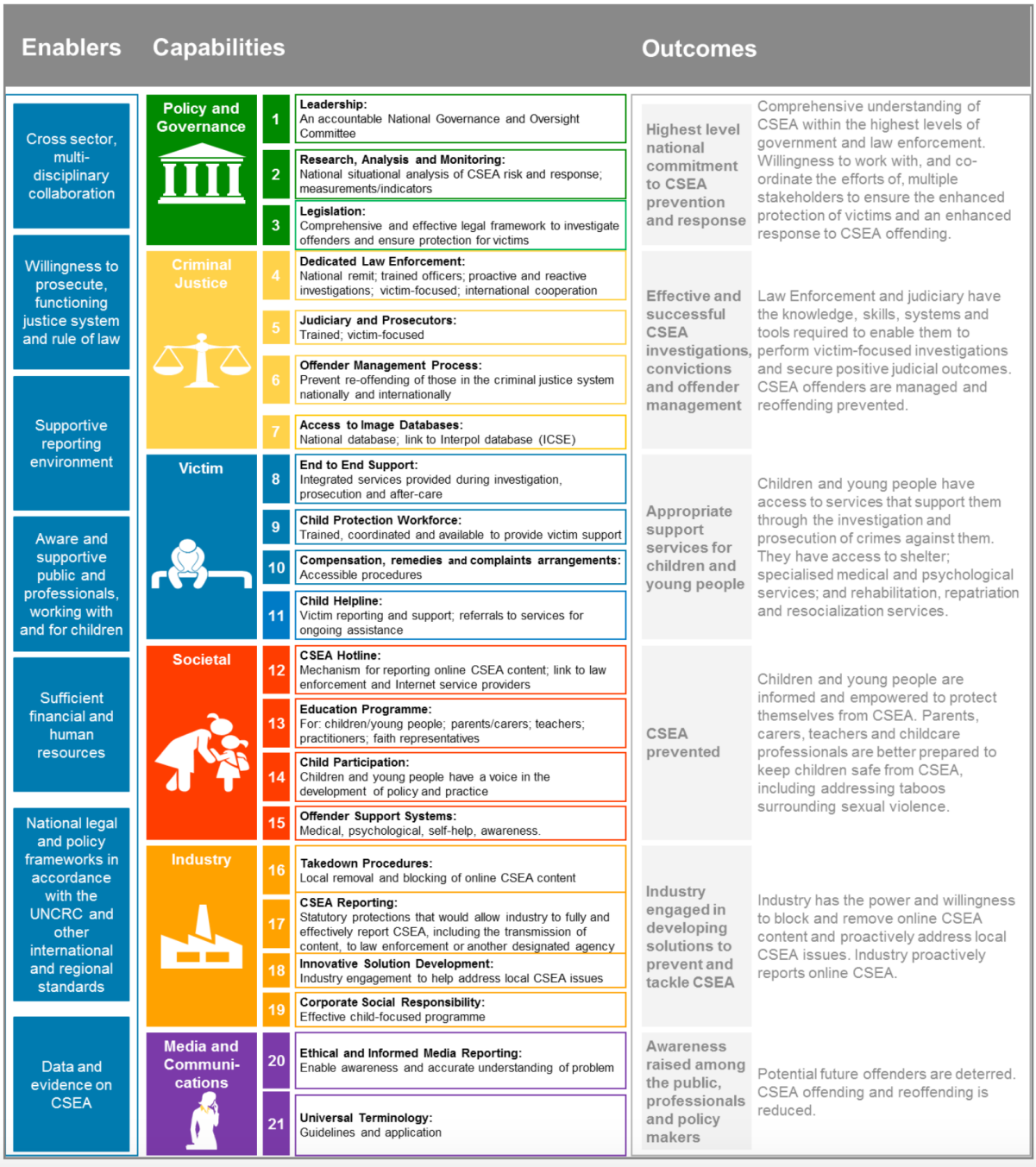
**UN SDG 3** Ensure healthy lives and *promote wellbeing for all at all ages*
**UN SDG 9** Industry, Innovation, Infrastructure: to develop quality, reliable, sustainable and resilient infrastructure to support economic development *and human wellbeing*
**UN SDG 11** Sustainable cities and communities – This should extend to *online communities*
**UN SDG 16** Promote peaceful and inclusive societies… accountable and inclusive institutions at all levels – (*SafeToNet observation: today social media companies are by law not accountable*). **16.1.4** Proportion of population that feel safe walking alone around the area they live (*SafeToNet observation: create safer spaces by implementing Contextual Safeguarding*). **16.2** End abuse, exploitation, trafficking and all forms of violence against and torture of children (*SafeToNet observation: this extends to all forms of violence in the online space*)

The UK Government published a consultative Online Harms white paper in early 2019, which is expected to lead to legislation in 2020, COVID-19 notwithstanding. While there are many commendable aspects to the proposals in the Whitepaper, it notably missed the opportunity to create a nationally recognised legal definition of the term, despite the fact that many activities that constitute cyberbullying are illegal. We note that this situation is paralleled in Australia and respectfully suggest that Australia leads the way in bringing about a legal definition if this term. It isn't suggested that the motivation is to criminalise perpetrators, more to underline the seriousness of this activity and to make it easier to teach young people about. Having said then in extreme cases where cyberbullying leads to suicide of the victim, some legal redress would be available to the victim's family.

Australia's Government and Australian organisations are members of the WeProtect Global Alliance (WPGA). WPGA has produced both a Global Strategic Response and a Model National Response (see below):



SafeToNet submission to the Australian Government's CCTIES




We believe that these frameworks provide ideal best practice approaches to dealing with the worst of the worse child sexual abuse imagery but other online harms as define by the EU Kids online project that span Contact, Conduct and Content – however there is limited engagement with tangible tech solutions or any measurable impacts or outcomes. Since perpetrators use the most sophisticated technology to commit these crimes why should governments not engage and deploy disruptive counter solutions?

Research shows that many online harms originate from conversations that children have online. We know from our own data the shockingly young age that girls in particular are engaging in conversations of a sexual nature. We know that the prime tool used in the practice of grooming, whether for sexual exploitation or for radicalisation, is a smartphone and a conversation. SafeToNet's AI-based real time safeguarding and wellbeing solution helps to disrupt these conversations, often preventing them from continuing, and preventing the harm from being done.

We would welcome the opportunity either through SafeToNet or our charitable Foundation to discuss a number of innovative ways the Australian Government can work with us to better safeguard Australia's children.