# UK “Secure by Design” vs Australian “Safety by Design”

**By Kruakae Pothong and Sonia Livingstone**

While the Covid-19 pandemic has sent internet use to record levels among both children and adults, UK household adoption of connected devices has been growing steadily. The more digitally connected our lives are, the more our and our children’s safety depends on these technologies being safe to use within various social contexts. But, what does it take to be safe in the digital environment?

*Image credit: Katerina Holmes from Pexels*

National, regional and international organisations have rolled out measures to make our connected lives safe(r), ranging from technical solutions to voluntary codes of practice, security standards, privacy standards and digital regulations such as the UK Online Safety Bill and the European Digital Services Act. These measures generally take a broad-brush approach to protect users. Other guidelines specifically consider children’s evolving capacities in their recommendations. Examples include the Council of Europe IT Handbook for policymakers, the Broadband Commission’s Child Online Safety and the UN Committee on the Rights of the Child’s General Comment 25 on the digital environment.

These measures reflect key design principles: safety, security and privacy. Interventions to implement these principles are best made right from the start in the design process, thereby shaping product development early. This is certainly more effective than trying to retrofit a digital product or service after it has reached the market and safety, security, or privacy problems are identified. Hence the terms Safety by Design, Secure by Design and Privacy by Design. Given the nature of today’s agile framework for product innovation, these aspects of design should be iterated and integrated into all product development sprints.

In today's data-driven societies, very little goes unrecorded. Increasingly, safety, security and privacy are interlinked. For example, the recent cyberattack on UK schools (a security breach, resulting from VPN vulnerabilities, phishing emails, weak passwords for remote access) means that the attacker has access to personally identifiable information about children (a privacy breach). Such unauthorised access to information about children could result in children's overall safety risks.

So, safety, security and privacy each play a part in is protecting individuals. The difference between these three principles lies in their emphasis. As in the case of the Australian Safety by Design principles[1], the safety principle approaches online risks and harms from the social dimension of technology use, comprising content, contact, contract and conduct risks. According to the American National Institute of Standards and Technology (NIST), the focus on security and privacy principles protects users from a technical angle. Information Security focuses on risks resulting from loss of confidentiality, integrity and/or availability (of system and data) taking place within the information systems, while privacy focuses on the risks associated with data processing. Both security and privacy risks can, in turn, undermine children's online safety, exposing them to content, contact and conduct risks.

To illustrate these similarities and differences, compare the UK Department for Digital, Culture, Media and Sport (DCMS) Secure by Design Code of Practice with the Australian Safety by Design principles in operation.

| Key features | The UK Secure by Design | AUS Safety by Design |
|---|---|---|
| Application scope | Consumer IoT | Online products, services and platforms |
| Emphasis | Security (Technical protocols) of consumer IoT | Overall online safety, supported by security and privacy protocols |
| Apply to | All parties involved in the development, manufacturing and retail of consumer IoT | Providers of online products, services and platforms |
| Enforcement | Currently voluntary Code of practice | Voluntary |

The key differences lie in their application scope (only consumer IoT vs all online products and services) and emphasis (technical security vs sociotechnical safety). However, they are similar in the types of duty bearers they address – providers of the products and services in scope – and their current enforcement mechanism, which is voluntary.

The UK Secure by Design Code of Practice addresses the technical aspects of consumer products that connect to the Internet, also referred to as consumer Internet of Things (IoT), such as connected children's toys, baby monitors, smart speakers and wearable health trackers. It prescribes 13 practical steps for parties involved in the development, manufacturer and retail of consumer IoT to improve the security of their products and services which will, in turn, protect consumers' privacy and safety. The UK government is planning to mandate the top 3 principles of the Code so as to:

1. ensure that device passwords are all unique and not resettable to any universal usernames and passwords (e.g. 'admin', 'admin'),
2. make it easier for users to report software vulnerabilities and have them fixed,
3. require digital providers to declare the minimum period for which consumers can expect their device to receive security updates.

The Code also prescribes practical steps to protect users against risks arising from data processing, such as not writing usernames and passwords in the software and requiring secure storage as well as encryption of security-sensitive data in transit. These security-sensitive data include encryption keys, device identifiers, remote

management and control. In this way, the Code minimises the exploitation of technical vulnerabilities by cybercriminals but does not address other forms of exploitation by other types of social-economic actors.

The Australian Safety by Design, on the other hand, addresses online risks and harms from the social angle of digital technology usage and thus covers a broader spectrum of digital products and services. It addresses the sociotechnical challenges to safety by

1. prescribing clear responsibilities for digital providers, which include implementing technical measures to address security and privacy risks,
2. empowering users through user-centric design,
3. transparency and accountability to empower users.

Unlike the UK Secure by Design Code of Practice, the Australian safety by design principles is the product of the Enhancing Online Safety Act 2015, created to help businesses comply with the law and with children as focal.

Learning from available guidelines, protecting users in modern data-driven societies requires a comprehensive and holistic approach and involves engaging multiple stakeholders, from designers to digital providers, governments to end-users, to play ball. The Digital Futures Commission aims to combine the strength of these different approaches in support of children's rights and will develop practical guidance for innovators to embed children's rights at the heart of digital design and development processes. Our rationale is that human rights, including children's rights, provide a benchmark for how users and digital providers should treat one another, and General Comment 25 has made it clear that such standards should be coded into the way digital technologies, their providers and users operate.

Notes:

[1] The eSafety Commissioner Office is an independent statutory body responsible for promoting online safety for Australian citizens, as outlined in the Enhancing Online Safety Act (2015).

You can view the rest of the blog series here.

Professor Sonia Livingstone OBE is a member of the UNCRC General Comment's Steering Group, and leads the Digital Futures Commission. Sonia is Professor of Social Psychology in the Department of Media and Communications at the London School of Economics and Political Science. She has published twenty books on media audiences, media literacy, and media regulation, with a particular focus on the opportunities and risks of digital media for children and young people.

Dr Kruakae Pothong is a researcher at 5Rights and visiting research fellow in the Department of Media and Communications at London School of Economics and Political Science. Her current research focuses on child-centred design for digital services and children's education data. Her broader research interests span the areas of human-computer interaction, digital ethics, data protection, Internet and other related policies.

---

**Originally posted on https://digitalfuturescommission.org.uk/ on May 24, 2021 .**