IEEE SSIT SOCIETY ON SOCIAL IMPLICATIONS OF TECHNOLOGY

Society on Social Implications of Technology (SSIT) Australia Submission on 2023-2030 Australian Cyber Security Strategy Discussion Paper

April 2023

Authors (in alphabetical order)

Greg Adamson (University of Melbourne)
Mark Ames (Independent consultant)
Mark Brady (Charles Darwin University)
Elizabeth Englezos (Griffith University)
Samuli Haataja (Griffith University)
Ruth Lewis (Technology Foresight)

About us

The IEEE Society on Social Implications of Technology (SSIT) explores the social and ethical implications of technology, ensuring that IEEE fulfils its mission of advancing technology for humanity. With more than 400,000 members in 160 countries, IEEE is the world's largest technical professional association. SSIT is a community that engages some of the world's experts on technology and its impact, but also philosophers, lawyers, ethicists, policy makers – in general people who take an active interest in where humanity and emerging technologies are headed and can interact. The Australia Chapter (SSIT Australia) pursues a wide range of activities in the Australia region, including technical meetings, international conferences, and development of public policy through workshops and submission papers. SSIT Australia has members from a wide range of industries and academic backgrounds joining an ongoing dialogue on the social implications of technology. This submission has been prepared by members of SSIT Australia.[1]

Overview of submission

We appreciate the opportunity to contribute to the 2023-2030 Australian Cyber Security Strategy. Our submission reflects our views as researchers and professionals. They do not reflect the views of our institutions.

The main points of our submission are:

- The cybersecurity challenges associated with operational technology should not be ignored (Question 1);
- Australia should leverage existing international agreements with regional neighbours to develop cybersecurity (Question 3);
- Australia should further enhance its national position on how it considers international law to apply in the cyber context (Question 5);
- Australia should continue to participate in developing international standards (Question 5);
- Australia should not approach cybersecurity challenges from a purely STEM (science, technology, engineering and mathematics) perspective (Question 11);
- Australia should develop its cybersecurity workforce (Question 11); and
- Australia should consider the cybersecurity challenges associated with emerging technologies, such as automated driving systems; and those associated with social media platforms, and promote security by design (Question 19).

[1] For more information on SSIT Australia, see https://technologyandsociety.org/member-resources/find-a-local-ssit-group/australia-chapter/

The need for safety (Question 1)

The report provides a good examination of cyber challenges in the on-line world, but ignores cyber challenges in the physical world. A search for "safety" shows no attention to the threat to physical safety in the medical, transport or other sectors. In general, Operational Technology challenges are only slightly addressed. The Federal government is undertaking extensive protection of critical infrastructure, and this should be reflected in the report.

Building a Basis for Regional Cooperation (Question 3)

Australia has several existing agreements in place with our neighbours and other countries in the region in terms of trade, travel, policing, human rights reciprocity and several other areas. These relationships can be leveraged to agree a baseline on approach to cybersecurity across the region. A significant challenge will be in defining the scope and identifying the most likely areas for agreement, cooperation, and standardisation. Initial approaches, if not already in place, could include air traffic control and communications systems, telecommunications and other areas where significant agreements and cooperation covering safety and critical infrastructure are already in place.

Enhance Australia's position on how it considers international law to apply in cyberspace (Question 5)

With the aim of developing shared understandings about responsible state behaviour in the cyber context, Australia should further enhance its national position on how it considers international law to apply in this context.

Australia has previously recognised the application of international law in the cyber context, and outlined its position on a number of relevant areas of law. This was done in its 2017 International Cyber Engagement Strategy,[2] in a speech by then Attorney-General George Brandis in 2017,[3] in the 2019 International Law Supplement to the International Cyber Engagement Strategy,[4] in an annex to the 2020 International Cyber and Critical Technology Engagement Strategy,[5] and in its submission to the 2021 UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security.[6] Overall, these have been positive in their contribution to shared understandings about

[2] Department of Foreign Affairs and Trade, 'Australia's International Cyber Engagement Strategy' (October 2017) 47-48.

[3] George Brandis, 'The Right of Self-Defence Against Imminent Armed Attack in International Law' (Speech at University of Queensland, 11 April 2017) <https://law.uq.edu.au/blog/2017/05/developments-international-law-self-defence-against-imminent-armed-attack>.

[4] Department of Foreign Affairs and Trade, 'Australia's International Cyber Engagement Strategy, 2019 International Law Supplement' (2019) <https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019%20Legal%20Supplment_0.PDF>.

[5] Department of Foreign Affairs and Trade, 'International Cyber and Critical Technology Engagement Strategy, Annex B: Australia's position on how international law applies to State conduct in cyberspace' (2020) <https://www.internationalcybertech.gov.au/our-work/annexes/annex-b>.

[6] Australian Government, 'Australia's submission on international law to be annexed to the report of the

how international law applies to State activities in cyberspace, and are consistent with Australia's 2021 International Cyber and Critical Technology Engagement Strategy.[7]

However, in its 2023-2030 Cyber Security Strategy, Australia should further enhance its national position on how international law applies in cyberspace in both in substance and in form. In substance, Australia should articulate its position on the status and scope of relevant areas of law, such as sovereignty and due diligence, in more depth. In relation to sovereignty, Australia's position should confirm the application of 'sovereignty as a rule' that prohibits certain remotely conducted cyber operations that go beyond mere cyber espionage.[8] In relation to due diligence, Australia should confirm the customary international law status of the law which applies in the cyber context as it does in the non-cyber context.[9] In each of these contexts, as well as in Australia's position generally, references to relevant legal authorities should be provided to support Australia's position on the law. Examples of other States' positions that have done so include Germany where statements about the applicable law are supported by legal authorities.[10] In form, Australia's national position should be consolidated into a single document organised according to relevant areas of law. Recent others States that have published their national positions provide useful models of this, such as the national position of Canada published in 2022.[11] Overall, by further enhancing its national position on how international law applies in the cyber context, Australia will continue to contribute to setting shared expectations about responsible behaviour in this context.

Participation in the development of international standards (Question 5)

Technology standards in cyberspace often emerge from technology focussed standards bodies, including the IEEE Standards Association (Local Area Networks, Wi-Fi), Internet Engineering Task Force (Internet RFCs), and the World-Wide Web Consortium (world-wide web standards). The Australian government actively engages with IEEE Standards Association in several areas: the Australian Communications and Media Authority is a member of IEEE SA's Government Engagement Program on Standards,[12] the Australian Human Rights Commissioner's Report on Human Rights and Technology makes extensive reference to IEEE

2021 Group of Governmental Experts on Cyber' (2021) <https://www.internationalcybertech.gov.au/sites/default/files/2021-06/Australia%20Annex%20-%20Final%2C%20as%20submitted%20to%20GGE%20Secretariat.pdf>.

[7] Department of Foreign Affairs and Trade, 'Australia's International Cyber and Critical Technology Engagement Strategy' (2021) 36-41.

[8] See Anna-Maria Osula, Agnes Kasper and Aleksi Kajander, 'EU Common Position on International Law and Cyberspace' (2022) 16(1) Masaryk University Journal of Law and Technology 89, 95-99.

[9] See Antonio Coco and Talita de Souza Dias, 'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law' (2021) 32(3) European Journal of International Law 771.

[10] See The Federal Government of Germany, 'On the Application of International Law in Cyberspace' (March 2021) <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf>.

[11] See Government of Canada, 'International Law applicable in cyberspace' (22 April 2022) <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng>.

[12] https://standards.ieee.org/about/intl/government-engagement-program/

initiatives,[13] and there has been significant interest in IEEE's work on the digital rights of the child.[14] These examples show the practical engagement and influence which the Australian government is able to achieve in an important standards forum. Current IEEE SA cyber security clusters include:

Energy/Smart Grid**:** IEEE C37.240-2014 - IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems; IEEE 1686-2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities; IEEE P2030.102.1: Standard for Interoperability of Internet Protocol Security (IPsec) Utilized within Utility Control Systems; IEEE P1711 - Standard for a Cryptographic Protocol for Electric Power System (EPS) Communications Links; IEEE P1711.1 - Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links: Substation Serial Protection Protocol; IEEE P2658: Guide for Cybersecurity Testing in Electric Power Systems; IEEE 802.15.4-2020 - IEEE Approved Draft Standard for Low-Rate Wireless Networks. The IEEE 802.15.4 protocol is used in smart grid applications (smart metering) and has several security features such as access control, frame integrity, and confidentiality.

IEEE SA has initiated some key work on Blockchain Focused on Energy: IEEE P825 - Guide for Interoperability of Transactive Energy Systems with Electric Power Infrastructure (Building the Enabling Network for Distributed Energy Resources); IEEE P2418.5 - Standard for Blockchain in Energy. IEEE 692-2013, IEEE Standard for Criteria for Security Systems for Nuclear Power Generating Stations, developed by WG 3.2 – Security Systems Working Group, addresses security system equipment for "detection, assessment, surveillance, access control, communication, and data acquisition".

The numerous IEEE smart grid systems standards include a number focused on security, e.g. IEEE C37.240-2014 – IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems developed by 240 WG – PC37.240 Cyber Security Standard and IEEE 1686-2013 – IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities developed by WGC1 – Substations Working Group C1.

Healthcare/Wearables/Consumer: IEEE 11073 Series of Standards: IEEE 11703 has one part on cyber security for medical devices under the P11073-40101 - IEEE Draft Standard -Health informatics - Device interoperability - Part 40101: Cybersecurity - Processes for vulnerability assessment: IEEE P1912: Standard for Privacy and Security Architecture for Consumer Wireless Devices; IEEE 2621 Working Group: Standard for Wireless Health Device Security Assurance. There are 3 standards within this framework: IEEE P2621.1: Standard for Wireless Diabetes Device Security Assurance: Product Security Evaluation Program; IEEE P2621.2: Project Title: Standard for Wireless Diabetes Device Security Assurance: Protection Profile for Connected Diabetes Devices; IEEE P2621.3: Project Title: Standard for Wireless Diabetes Device Security Assurance: Guidance for Mobile Devices. IEEE PHD (Personal Healthcare Devices) Cybersecurity Standards Roadmap – Whitepaper; IEEE SA Pre-Standards

[13] https://humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-final-report-2021

[14] https://standards.ieee.org/news/ieee-2089/

Workstream Report: Clinical IoT Data Validation and Interoperability with Blockchain - White paper; IEEE P2933: Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS - Trust, Identity, Privacy, Protection, Safety, Security; IEEE 2410: IEEE Standard for Biometric Open Protocol; IEEE P2418.6 - Standard for the Framework of Distributed Ledger Technology (DLT) Use in Healthcare and the Life and Social Sciences.

FinTech: IEEE P1940: Standard Profiles for ISO 8583 Authentication Services. IEEE P1940 is mainly focused on financial transactions (e.g., point-of-sale (POS), automated teller machine (ATM) cash withdrawal transactions, etc.). Such services include biometric authentication (as defined by IEEE Std. 2410), PIN-based, Fast Identity Online (FIDO), and One-Time Password (OTP) and Time-based OTP (TOTP) authentication methods including risk and presentation attack defense (PAD) measures.

Software: IEEE Computer Society Cybersecurity and Privacy Standards Committee: IEEE 1619 series on crypto protection for storage devices; IEEE 1619-2018 - IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices; IEEE 1619.1-2018 - IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices; IEEE P1619.2 - Standard for Wide-Block Encryption for Shared Storage Media. IEEE P2883 - Standard for Sanitizing Storage; IEEE 1667-2018 - IEEE Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices; IEEE P2986: Recommended Practice for Privacy and Security for Federated Machine Learning (C/AI); IEEE P2994: Standard for Security Assessment Framework for IoT Application Deployments (COM/Mobile)

Mobility/Automotive: IEEE P1609.2: Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages.

IEEE 802 standards: The IEEE 802.1AE standard defines a Layer 2 security protocol called Medium Access Control Security (MACSec) that provides point-to-point security on Ethernet links between nodes for securing wired LANs. IEEE 802.11 standard also includes security features that include: Service Set Identifier (SSID) which is used to control access to an Access Point (AP), the Access Control List (ACL) to prevent unauthorized access, and the Wired Equivalent Privacy (WEP) protocol: IEEE 802.11bh: Operation with Randomized and Changing MAC Addresses (LAN/MAN); IEEE 802.11bi: Enhanced Service with Data Privacy Protection; IEEE 802E: Privacy.

IEEE Standards on Blockchain: IEEE has 30-40 standards focused in the area of Blockchain, many focus on the key aspects of security. IEEE Blockchain & Distributed Ledger Standards Committee: IEEE P3200 series of standards are being developed within this committee focusing on identity, interoperability, and security (there are about 10 standards in the IEEE 3200 series).

IoT Framework Standards: IEEE 2413-2019, Standard for an Architectural Framework for the Internet of Things.

SSIT Standards on ethical and safe use of emerging Technology: IEEE Society for Social Implications of Technology Standards Committee has many standards under development which promote the safe benefits of development, use and operation of current and emerging technology and data, whilst minimising the risks. This Standards Committee offers significant Australian contribution to international standards-setting, as Standards Committee Officers are in Australia. Developing standards include IEEE P2895 Standard Taxonomy for Responsible Trading of Human-Generated Data, IEEE P2987 Recommended Practice for Principles for Design and Operation Addressing Technology-Facilitated Inter-Personal Control, IEEE P7012 Standard for Machine Readable Personal Privacy Terms, P7014 Standard for Ethical Consideration in Emulated Empathy in Autonomous and Intelligent Systems, P7030 Recommended Practice for Ethical Assessment of Extended Reality (XR) Technologies, P7700 Recommended Practice for the Responsible Design and Development of Neurotechnologies and P7016 Standard for Ethically Aligned Design and Operation of Metaverse Systems.

Beyond the STEM agenda (Question 11)

The great majority of cyber security attacks begin with social engineering, which is not a STEM field. An expectation that technology is the solution to cyber security will be entirely technical has no basis in experience. SSIT Australia is actively involved with the IEEE Standards Association initiative Meta Issues in Cybersecurity.[15] This industry engagement initiative is examining cyber security from several perspectives, illustrating best practice in addressing high level challenges to the ongoing challenge of cyber security:

1. Economics of cyber security
2. Psychology/human behavior and cyber security
3. Legal aspects of cyber security
4. Public policy and cyber security
5. Technical aspects of cyber security
6. Cyber security and policing
7. Cyber security and insurance standards

Supporting Australia's cyber security workforce (Question 11)

In order to address the challenge for Australia, we should understand the global challenge and how we can address this. If Australia is to be a leading cyber security nation by 2030, we cannot simply depend on professional immigration. Rather, we should see this as an opportunity to provide services to our region and beyond. According to widely cited research, there is a global cyber security workforce of around 3.5 million in 2021, which represented a shortfall of around 3 million people.[16]

The challenge is more than just training more people in an established field. It is helping the field itself establish. The IEEE Standards Association initiative Meta Issues in Cybersecurity

[15] https://standards.ieee.org/industry-connections/meta-issues-cybersecurity/
[16] https://www.weforum.org/agenda/2021/05/cybersecurity-governments-business/

has prepared a report that the solution to this shortfall involves promoting the profession of cyber security.[17] IEEE itself was founded in 1884, and first adopted a Code of Ethics in 1912. Other organisations also have long histories of professionalism in areas related to cyber security. The report's executive summary recommends that IEEE contribute to the strengthening of the cyber security field in four ways:

> The cyber security problem: Dependence on technology is growing, particularly since the COVID-19 pandemic. Yet safe use of technology depends on cyber security, which is failing to keep up. This failure can derail global benefits that humanity should achieve from cyberspace and its technologies.
>
> Why this matters to IEEE: Some 4 million professionals work in the cyber security field. IEEE could play a major role in this global community, and in addressing the growing cyber security threat, based on four strengths: IEEE's commitment to advancing technology for humanity; its global presence and independence; its engagement across the technology "stack"; and its experience in both cyber research and industry.
>
> This report reviews the IEEE experience and its potential role in the global cyber security community. We welcome feedback and improvements for future updates to report.
>
> Recommendations
>
> 1. Purpose
>
> Attacks on cyber security are attacks on the safety of cyberspace itself, and on the benefits humanity can achieve from this enormous field of technology.
> Recommendation 1: IEEE should link the dependency with cyber security to the achievement of our goal of advancing technology for humanity.
>
> 2. Independence
>
> IEEE has members in 160 countries. Most people in the world benefit from our standards every day. We promote beneficial use of technology generally, not narrow national or commercial interests.
> Recommendation 2: IEEE should apply its reputation for independence to establishing cyber security principles and standards which make all technologies more trustworthy.
>
> 3. Breadth
>
> Advanced technologies are less predictable, isolated, and mechanical, more intelligent, distributed, and social. IEEE members are found in all these fields, from power to quantum to societal.
> Recommendation 3: IEEE should encourage a holistic approach to cyber security, not just the obvious vulnerabilities, reflecting the breadth of its members' expertise.
>
> 4. Experience
>
> IEEE publishes three of the top four cyber security journals, has many standards, conferences, and educational activities, and many thousands of members working in the industry.
> Recommendation 4: IEEE should use its areas of deep experience to encourage cyber security specialists to make IEEE their professional home.

[17] https://standards.ieee.org/industry-connections/meta-issues-cybersecurity/

Cybersecurity in emerging technologies (Question 19)

Australia should consider the cybersecurity challenges associated with emerging technologies, such as automated driving systems; and those associated with social media platforms.

As autonomous road vehicles become more prevalent on Australian roads the potential for interference with their automated driving system (ADS) increases. As a corollary of that, so does the potential to disrupt Australian society by malevolent state or non-state actors in future. While computer offences are covered in within the Commonwealth Criminal Code,[18] the Code deals principally with computers owned and operated by the Commonwealth. For example, under division 477.3,[19] 'a person commits an offence if the person causes any unauthorised impairment of electronic communication to or from a computer and the person knows that the impairment is unauthorised.[20] An amendment to deem the ADS of an autonomous vehicle as 'restricted' (with reasonable exceptions for maintenance etc) would go some way towards addressing the cyber security of autonomous vehicles in Australia as it would bring interference with such systems under the purview of the Commonwealth Criminal Code and thereby act as a partial deterrent against interference.

Additionally, some consideration may need to be given to the data transmitted to and from automated driving systems when communicating with infrastructure and other vehicles. Currently, telecommunications are covered under division 474.14 'interference with a telecommunications network' where a person 'connects equipment to a telecommunications network,[21] and 'intends to commit, or to facilitate the commission of a serious offence against Commonwealth, state or foreign law'. An amendment to the Criminal Code to include interference with communications to and from autonomous vehicles within the definition of serious offence would also act as a partial deterrent to interference with such systems.

The above example considers one of the many targeted ways in which discrete or purpose-orientated data can be misused and operationalised to produce harm. In such cases, interference can occur in ways that are related to the original purpose of data generation. Social media platforms, search engines and large-scale data processors present a particular challenge for government regulation given their vast access to data and their expansive role in the lives of Australians. While consumers and government entities have become increasingly aware of the potential threat posed by those processing otherwise 'innocuous'[22] data, the fact remains that the average individual produces 1.7MB of data per second (and thus more than 146GB per day).[23] The conduct of digital platforms carries substantial consequence for Australians as they

[18] *Criminal Code Act 1995* (Cth) Part 10.7.

[19] *Criminal Code Act 1995* (Cth) s 477.3.

[20] *Criminal Code Act 1995* (Cth) s 477.3(1).

[21] *Criminal Code Act 1995* (Cth) s 474.14(1)(a)(i).

[22] 'Innocuous' here only refers to data which appears unimportant or frivolous in nature, rather than data that has obvious consequence or value.

[23] Jordan T. Prodanoff, 'How Much Data is Created Everyday in 2022' *Webtribunal.net* (Blog post, 7 October 2022) https://webtribunal.net/blog/how-much-data-is-created-every-day/#gref.

have often become so embedded with day-to-day life that they now serve infrastructural purposes.[24] An important case in point is the recent decision to ban the use of TikTok on Australian Government devices (’TikTok ban’).[25] While the Australian government’s position echoes measures taken by other nations with in the Five Eyes Alliance,[26] it departs from concerns based on international influence through social media due to its focus on data and (cyber)security concerns. In the instance of government agencies and the sensitive information available through existing protections (as envisaged and putatively addressed by the TikTok ban) we cannot rely on the protection of information[27] to protect against cybersecurity threats. Data must also be protected.

We have seen algorithms commonly applied to problematic ends. The recent Productivity Commission Inquiry into Centrelink’s Online Compliance Initiative (otherwise known as ’Robodebt’) provides an important case in point as to how data or information can be mishandled – even where the intent is to achieve a positive outcome. However, raw data can also be used to draw discriminatory and highly problematic inferences.[28] The training of this data based on Machine Learning models and (potentially) combined with Artificial Intelligence[29] can be operationalised to infer information and characteristics about an individual that are not reasonably foreseeable based on the data alone.[30] The matter of Cambridge Analytica and the threats posed by digital platforms has been written about at length. However, the capacity to influence people based on inferences about their beliefs or values is likely to be the *tip* of the iceberg. Such influences may not remain covert. For example, inferences about sexual orientation or those infer sensitive details Australian citizens may leave those persons vulnerable to extortion or blackmail. To that end, cybersecurity measures must address the way data can be operationalized and potentially weaponized through the use of these techniques and that protects against the use of data to infer private characteristics, traits or matters relating to the individual.

[24] See, for example, Fransen-Taylor, P. & Narayan, B. (2016). #Homeless but at home in cyberspace In *Proceedings of ISIC, the Information Behaviour Conference, Zadar, Croatia, 20-23 September, 2016: Part 1. Information Research, 21*(4), paper isic1610 <http://InformationR.net/ir/21-4/isic/isic1610.html>, for their discussion of the importance of social media as a way for the homeless to maintain contact with others.

[25] The Hon Mark Dreyfus, ‘TikTok ban on Government devices’, (Department of the Attorney-General, Media Release, 4 April 2023).

[26] Anastasia Santoreneos, ‘Australia bans TikTok on official devices: Attorney-General confirms’, *Forbes Australia* (online, 4 April 2023) <https://www.forbes.com.au/news/investing/tiktok-banned-australia-government-devices/#:~:text=India%20banned%20TikTok%20in%20June,implemented%20a%20ban%20on%20TikTok>.

[27] The term information is used here to refer to data that has some form of context that gives that data meaning. For example, a nine-digit number (alone, and without more) is data, as the number has no relevance without its context. However a nine-digit number that has a connection to the Australian Tax Office should be considered ‘information’ as it carries additional meaning that can be inferred from additional details or context.

[28] See, Elizabeth Englezos, ‘Policing by Algorithm: NSW Police’s Suspect Target Management Plan’ (2023) 48(1) *Alternative Law Journal* 17, for a discussion of algorithmic predictions and the subsequent increased targeting of indigenous youth.

[29] Both generative (such as ChatGPT) or otherwise.

[30] See, for example, Renaud Lambiotte and Michael Kosinski, ‘Tracking the Digital Foptprints of Personality’ (2014) 102(12) *Proceedings of the IEEE* 1934, which discusses the use of ‘big social data’ to predict the personality traits of individuals.

Protecting the use of data to create private inferences about a person.

To future-proof cybersecurity measures, regulations and prohibitions must also address the use of data processing techniques that *infer* what would otherwise be ‘private information’ or perhaps ‘confidential information.’ Guidance as to what constitutes confidential information could be drawn from the equitable doctrine breach of confidence.[31] In the 2001, High Court definitively ruled against a right of privacy in Australia.[32] However, the High Court acknowledged that ‘where the information in question has been obtained illegally, tortiously, surreptitiously or improperly, even where the possessor is itself innocent of wrongdoing’ the court would have jurisdiction to intervene to ‘restrain the use of confidential information.’[33] Confidential information about a person is therefore worthy of protection, regardless of its source.

Case law has provided further advice as to what constitutes confidential information. According to the landmark case of *Coco v A N Clark (Engineers) Ltd* (‘*Coco v Clark’*) information can be considered confidential where:

1. The information has a necessary quality of confidence, and
2. The information was imparted in circumstances importing an obligation of confidence.[34]

Inferences based on such data or information should also be considered confidential. Where the aforementioned requirements are met, the disclosure of these inferences should constitute a breach of confidence,[35] and should include inferences that are that is not common knowledge and/or not freely available in the public domain.[36] It is important to note that in *Coco v Clark*, a third element required that the information is disclosed without authorisation. However, in the case of inferences – there is no similar opportunity for the individual to ‘authorise’ the disclosure of this information. To balance this absences, further guidance could be taken from:

1. the steps taken to restrict the disclosure of (or access to) that information, and
2. balanced on common ideals such as internationally recognised privacy ideals such as the ‘right to be let alone’[37] or protection against ‘intrusion upon seclusion’[38] or for ‘public given to private life’.[39]

While we cannot predict how technology will develop in the future, algorithms, AI and machine learning will remain a fundamental part of our digital dealings. Protecting individual data, and preventing the application of digitally-enabled inferences about the individual

[31] See, *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] 208 CLR 199.

[32] Ibid [74].

[33] Ibid [170].

[34] *Coco v A N Clark (Engineers) Pty Ltd* (1968) 1A IPR 587, 590-591 (‘*Coco v Clark*’).

[35] Ibid 591.

[36] Ibid 590.

[37] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, 195.

[38] See also the United States’ Restatement (Second) of Torts §§ 652B b. which also includes the use of ‘mechanical aids to oversee or overhear the [person’s] private affairs… [or] some other form of investigation or examination of his private concerns’.

[39] This is outlined further in United States’ Restatement (Second) of Torts §§ 652D b. This refers specifically where the ‘facts’ are part of the private life and *not the public life* of the individual.

provides a strategy that addresses current cybersecurity challenges and remains adaptable to future technological developments.

Security by Design.

The Strategy should evolve to address the cyber security of emerging technologies and promote the practical use of security by design in new and emerging technologies. A way to do this is to recommend use of the international standards developed and published by IEEE Standards Association. These provide auditable recommendations and best practices on how to include ethics, security and compliance by design within new and emerging technologies. Of these, published standards such as ISO/IEC/IEEE 24748-7000:2022 Systems and software engineering — Life cycle management — Part 7000: Standard model process for addressing ethical concerns during system design, Standard 7002-2022 - IEEE Standard for Data Privacy Process, (which includes full lifecycle considerations of privacy by design at the organisational and system level), 7001-2021 - IEEE Standard for Transparency of Autonomous Systems, and Standard 7005-2021 - IEEE Standard for Transparent Employer Data Governance should be considered.

Developing standards that include ethics and security by design are P7700 Recommended Practice for the Responsible Design and Development of Neurotechnologies, P7016 Standard for Ethically Aligned Design and Operation of Metaverse Systems and P7030 Recommended Practice for Ethical Assessment of Extended Reality (XR) Technologies and IEEE P2987 Recommended Practice for Principles for Design and Operation Addressing Technology-Facilitated Inter-Personal Control. These developing standards will provide the Strategy with specific methods and tools to enable security by design.

Beyond security by design, emerging technologies should be designed, developed, deployed, monitored, governed, and decommissioned in a manner that respects and enables trustworthiness through privacy, accountability, transparency and mitigation of algorithmic bias. The Strategy should consider a recommendation of self-verification as well as third-party verification and certification of emerging technologies for trustworthiness and security. IEEE offers the IEEE CertifAIEdTM as a third-party certification program for assessing ethics and security of Autonomous Intelligent Systems (AIS) to help protect, differentiate, and grow product adoption in a trustworthy manner. Through certification guidance, assessment and independent verification, IEEE CertifAIEd offers the ability to scale responsible innovation implementations, thereby helping to increase the quality of AIS, the associated trust with key stakeholders, and realizing associated benefits. Certification is currently available in privacy, algorithmic bias, accountability and transparency. Transparency means that an emerging technology is operating in a way that is easy for others to see what actions are performed and why. Accountability requirements are essential to ensuring products, services, and systems are not harmful to society and consumers, and that risk of harm will be mitigated with humans being held accountable and/or legally responsible.