Charles Sturt University

Charles Sturt University Submission – Strengthening Australia's cyber security regulations and incentives

August 2021

Charles Sturt University

Office of the Vice-Chancellor

27 August 2021

Michael Pezzullo AO
Secretary
Department of Home Affairs
4 National Circuit
Barton ACT 2600

'Strengthening Australia's cyber security regulations and incentives' discussion paper

Dear Secretary

Charles Sturt University welcomes the opportunity to provide input to the Department of Home Affairs for its consultations on strengthening the cyber security of Australia's digital economy through regulatory reforms and voluntary incentives.

Charles Sturt University is Australia's largest regional university, with more than 43,000 students and approximately 2,000 full time equivalent staff. We are a unique multi-campus institution with campuses in some of New South Wales' fastest-growing and most vibrant regional communities, and strong connections to surrounding rural and remote communities.

Education at Charles Sturt has a strong focus on practical outcomes, as shown by our consistently high rankings for graduate employment and graduate starting salaries. This focus flows through to much of the research conducted at the University, with translation into concrete outcomes a key goal. The same philosophy informs our engagement with Australian and NSW Government consultations on a wide range of issues, including cyber security.

Charles Sturt has demonstrated expertise in cyber security and related fields including law, justice and security, information sciences and technology, and ethics. The University offers undergraduate and postgraduate programs in cyber security, and we are developing a Cybersecurity and Applied Data Research Institute (CARDI) at our campus in Bathurst. CARDI will draw on the existing capabilities across Charles Sturt, an established relationship with the NSW Government and a growing array of industry partners to provide a locus for collaboration in cyber security research, innovation and commercialisation.

Charles Sturt's submission to the 'Strengthening Australia's cyber security regulations and incentives' discussion paper has been developed by Professor Seumas Miller, Professor of Philosophy, and Dr Marcus Smith, Senior Lecturer in Law, both from the Australian Graduate School of Policing and Security. Professor Miller and Dr Smith can provide the Department of Home Affairs with further information on any of the issues addressed in our submission.

Yours sincerely

[redacted]

Professor John Germov
Interim Vice-Chancellor

‘Strengthening Australia’s cyber security regulations and incentives’ discussion paper

Charles Sturt University welcomes the opportunity to provide input on options to strengthen the cyber security of Australia’s digital economy through regulatory reforms and voluntary incentives.

This submission has been prepared by two researchers with expertise in the regulatory and ethical dimensions of cyber security: Professor Seumas Miller, Professor of Philosophy, and Dr Marcus Smith, Senior Lecturer in Law, both from the Australian Graduate School of Policing and Security.

Professors Miller and Dr Smith are co-authors of *Biometric Identification, Law and Ethics*, a forthcoming publication from Springer AG. Professor Miller is a co-author of *The Ethics of Cybersecurity*, to be published this year by Oxford University Press. Dr Smith is a co-author of *Technology Law: Australian and International Perspectives*, to be published in October by Cambridge University Press.

Professor Miller and Dr Smith can provide the Department with further information on any of the issues discussed below.

1. **What are the factors preventing the adoption of cyber security best practice in Australia?**

2. **Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?**

3. **What are the strengths and limitations of Australia’s current regulatory framework for cyber security?**

As the *Strengthening Australia’s Cyber Security* discussion paper acknowledges, cyber security is becoming an increasingly important issue for the Australian community and there is a need to take further steps to enhance it–this need is highlighted by the regular examples of cybersecurity breaches occurring[1].

In addressing the first consultation question, we believe there are four key factors preventing the adoption of cyber security best practice in Australia:

- first, the complexity of information and communication technologies and the fact that law and policy makers may not fully appreciate the implications of new technologies, including the associated data security risks;

- second, the pace at which the field is moving, and the time required for government to coordinate and implement effective responses, so that by the time measures are implemented, they may be obsolete and ineffective;

- third the internationalisation of the technology sector and the way the internet allows companies (and bad actors) to operate internationally across legal borders and regulatory regimes, compounded in some cases by their size and dominance in the market[2];

[1] See e.g. Evelyn Manfield, How Did the Cyber Attack on Nine and Parliament House Happen?, *Australian Broadcasting Corporation News*, 30 March 2021.
[2] Marcus Smith and Gregor Urbas, *Technology Law* (Cambridge University Press, 2021), Chapter 1.

- and fourth (and related to the first three factors) the so-called 'human factor', e.g. lack of awareness of cyber threats, reluctance to comply with cybersecurity measures[3].

Developments in one jurisdiction rapidly have international ramifications, due to the connectedness facilitated by the internet and modern communications technology. New technology creates challenges, because when it becomes available, new regulatory gaps arise.

For example, the emergence of cryptocurrencies required governments to legislate to clarify whether they constitute forms of currency, and whether they are subject to taxation and corporate finance laws. Another example is the need for privacy and data security law to develop to incorporate new forms of data, such as the creation of facial recognition templates from photographs uploaded to the social media platforms; and the challenges associated with regulating this data when it is held offshore by a company offshore.

There are the problems for Australian businesses and consumers arising from anonymity. Anonymity can provide protection to those engaged in unlawful activity on the Internet. More broadly, from a regulatory standpoint, cyberspace and the internationalisation of the internet has disrupted traditional state-based sovereignty – physical borders have become inconsequential as individuals and information can move between them instantaneously[4].

Another feature of the cybersecurity landscape in Australia is far less complex but, nevertheless, both pervasive and problematic, namely, elementary cyber security failings at the human or social level. As the Discussion paper notes, compliance with the European Telecommunication Standards Institute[5] baseline standard on smart devices (ESTI EN 303 645) is, at present, voluntary in Australia[6]; however, the government is considering mandating it[7]. We believe this would be a positive development and the benefits of reduced vulnerability outweigh the risks such as reduced product availability, and it is important that Australia, at a minimum, implement standard that are equivalent to Europe and the United Kingdom[8]. Further, we strongly believe it should be mandated in full, as opposed to only the top three requirements. Australia should not maintain lower standards that may lead to it being viewed as softer target in comparison with equivalent advanced economies around the world.

However, there are even more basic measures that could be implemented. We note, for example, the European Union Agency for Network and Information Security standards in relation to passwords for end users and service providers, that could be updated and mandated in Australia[9].

We offer the following suggestion in relation to passwords as a small-scale instance of the kind of government enabled infrastructure that is possible. Today we are required to manage tens or even hundreds of passwords: banks, online services and stores, government facilities and so on. This deluge leads to weak passwords, passwords written and stuck in a supposedly hidden place, such as under the desk, or ad hoc (and often weak) home-grown solutions such as keeping a list of files in a password-protected document. The situation is made worse by organisations sometimes

---

[3] Terry Bossomaier, Steve D'Alessandro and R. H. Bradbury *Human Dimensions of Cybersecurity* (CRC Press, 2019).
[4] Smith and Urbas op.cit., Chapter 2.
[5] European Standard ETSI EN 303 645 V2.1.1 (2020-06).
[6] *Strengthening Australia's Cyber Security Regulations and Incentives,* 30.
[7] Ibid, 32; Question 12, 34.
[8] United Kingdom Department for Digital, Culture, Media and Sport 2018, *Code of Practice for Consumer IoT Security*.
[9] European Union Agency for Network and Information Security, *Basic Security Practices Regarding Passwords and Online Identities* (2014).

requiring frequent password changes. The last example is the methodology behind one of the most secure solutions to password proliferation, the *password safe*. This is just an encrypted database, accessed through a single master password. The challenge of finding a good password safe is considerable. However, the Australian or State Governments, through one of their cyber entities, could select, maybe by tender, and endorse a password safe and make this easily available, akin to the COVID-19 check-in apps. Once downloaded the user would enter a strong master password, which, of course, would not be shared with the government, software designers or, indeed, anybody else.

4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

System Architecture and Legal Frameworks

Our own focus here is not on discrete technical measures and standards but rather on system architecture and legal frameworks. An important approach to technology regulation and cybersecurity described in the literature that seeks to address regulation and data protection challenges in this area, is the use of system architecture as an approach to regulation, in combination with traditional approaches such as law enforced through sanctions such as fines and imprisonment, or market settings. Some theorists refer to 'law' imposed by technological capabilities and system designs, rather than, or in combination with legally proscribing activities by legislation[10].

There are examples of such approaches being developed in Australia and other countries already. System architecture to regulate smart contracts and digital currencies is being implemented by government to provide the foundation for blockchain to become a mainstream part of the future private sector, providing authentication, security and auditability for digital currency transactions, and throughout the lifecycle of smart contracts. A consortium between the government and private sector is establishing the Australian National Blockchain to enable businesses to digitally manage contracts, exchange information and conduct authentication[11]. We note the *Strengthening Australia's Cyber Security* discussion paper states that cyber security is a shared responsibility between government, businesses and individuals, and critical infrastructure developed in concert with the key stakeholders is more likely to be effective.

Multimodal regulatory models, which combine system architecture and legal frameworks to both facilitate and limit the way technologies can operate, and regulate how data can be stored and transferred, are more likely to be successful than those that rely solely on law and sanctions, such as prescribing how technology companies operate and how they should store and transfer data. Establishing national infrastructure for companies to use would be of great benefit in mitigating the security issues associated with data being stored by multiple companies, across different national and international jurisdictions, using different infrastructures. It would of course need to be complemented by legal frameworks and operated by a trusted statutory authority[12].

The recent developments described above that are being implemented in relation to national infrastructure for contracting with blockchain technology could be adopted more broadly in relation

[10] See e.g. Lawrence Lessig, *Code* (Basic Books, 2006).
[11] Department of Industry, Science, Energy and Resources, *National Blockchain Roadmap* (Australian Government, 2020).
[12] Marcus Smith, 'A Modern Approach to Regulation: Integrating Law, System Architecture and Blockchain Technology in Australia' (2020) 48 *Australian Business Law Review* 460.

to other forms of technology and data to improve cybersecurity in Australia. Below we consider two areas of concern and possible responses to them.

Anonymity and the Role of a Statutory Authority

An important cybersecurity area of concern pertains to storage of, and access to, the email, social media etc. accounts of businesses and customers and, in particular, to on-line anonymity as an enabler of fraud, identity theft, etc. in the course of on-line business transactions. This calls for a reduction in anonymity yet somehow simultaneously preserving privacy and data security. One potential approach involving the establishment or use of an existing statutory authority is as follows[13].

Firstly, phone, email and social media account holders engaged in business transactions (as opposed to, for instance, private communication), i.e. businesses and their customers, are required to register with an independent statutory authority. The authority issues a unique identifier based on the driver's licence, passport etc. provided by these account holders. Phone companies, internet providers, social media platforms etc., including those based overseas, e.g. in the US, are required by law only to provide accounts to Australian businesses and customers who have registered with the statutory authority.

Secondly, the authority must provide to law enforcement under warrant the identity of those persons who breach laws. There is no anonymity for lawbreakers and, as a result, many will be deterred from engaging in unlawful behaviour in the context of on-line business transactions and, if not deterred, they are at risk of being identified, arrested, and charged (including under extradition provisions if they live overseas). Thirdly, to enhance cyber security, both in terms of user privacy and ability to deter or track criminals, a public-private key escrow system is put in place.

Under this escrow system arrangement, when the user generates a public-private key pair, the public key is uploaded to the statutory authority. A person, Jones, communicating as user U1, provides identifiers, e.g. name, Medicare number, electoral role address etc. Some sort of authentication process is needed to ensure that Jones did indeed upload the public key for U1. The statutory authority has a public website from which any business or would-be customer can download U1's public key and thus verify that a communication was indeed from him and not somebody using his identity in some way.

Now Jones can still communicate anonymously as U1. But if he breaches laws his identity can be revealed by the statutory authority to law enforcement (under warrant). Under this arrangement neither businesses nor phone companies, internet providers or social networks have any verified data as to who U1 really is. Only the statutory authority has this information and it is, presumably, very secure.

Now consider a dating site, i.e. a business providing a service to customers. Suppose user, U2, posts his profile and user, U3 likes it. U3 checks the signature on U2's profile and his messages against his public key from SA. She knows that U1 did actually sign the messages. When U3 subsequently goes missing after, according to her flatmate a new date, the police will be able to gain access to determine U2's identity. However, the situation in which U3 could obtain U2's identity before meeting up with him might be restricted. What U3 wants is the security that U2's identity could be revealed to law enforcement or possibly other agencies should need arise. Also,

[13] Seumas Miller and Terry Bossomaier, *The Ethics of Cybersecurity*, Oxford University Press, 2021 (forthcoming).

suppose the dating agency website is hacked; it now contains no personal information regarding the identity of its users.

Recommendation 1: The government should seek to reduce online anonymity in business transactions and, thereby, unlawful activity, while simultaneously protecting privacy, by providing a mandatory registration system for businesses and customers transacting on the internet. The registration system should be established under the aegis of a statutory authority and should be protected by a public-private key escrow mechanism.

Improving the Security of Biometrics

A key form of data in relation to cybersecurity, which is growing in importance and constitutive of the identity of Australian citizens is biometric identification templates. Biometrics is increasingly being used as a standard identifier for the verification and security of online transactions. This development is not necessarily welcome; indeed, perhaps it should even be resisted. For one thing, there are considerable privacy/autonomy issues in relation to a person's control of his or her biometric data[14]. For another, biometrics are not invulnerable. Biometric template databases can, of course, be hacked and biometric templates stolen or destroyed. However, there is also the possibility that a stolen biometric template could be used as a false identifier of a person. It is already possible to 3D print a fingerprint based on a biometric template of a person's fingerprint. However, given that one cannot change one's fingerprint or other biometric features, as one can change at will one's password, once biometrics are compromised, there is potentially a very significant downside. For instance, one or more criminals might come to be in possession of an apparently very reliable biometric, but in fact false, identifier of you which you cannot change or easily retrieve.

Nevertheless, given that biometrics, like it or not, are increasingly being used as a standard identifier, a question arises as to the storage of, and access to, biometric identification templates. There are a number of potential arrangements that could be explored here, including storing all biometric templates used for identification purposes in a centralised system under the aegis of a statutory authority rather than in private sector storage systems or seeking to largely obviate the need for storage of biometric templates by recourse to other identification methods, e.g. by storing and comparing only derived hash values[15]. Whatever the means by which the specific problem of storage of, and access to, biometric identification templates is ultimately to be addressed there is, we suggest, a need for a biometrics commissioner.

The Office of the Australian Information Commissioner (OAIC) has broad authority in the area of biometric information. Biometric information is used by the private sector, government, law enforcement and other organisation for security purposes. It is unclear whether the OAIC has the resources and specialist knowledge of biometrics to provide effective oversight of new developments. At present in Australia, no independent, specific oversight mechanisms exist to oversee or regulate the collection, retention and use of biometric information.

In overseas jurisdictions, independent statutory commissioners have been appointed and demonstrated a capacity to respond to concerns relating to consent, retention and use of biometric information.

[14] Marcus Smith and Seumas Miller, *Biometrics, Law and Ethics*, Springer, 2021 (forthcoming)
[15] Miller and Bossomaier, *The Ethics of Cybersecurity* op. cit.

For example, the United Kingdom has created a Commissioner for the Retention and Use of Biometric Material (UK Biometrics Commissioner). The UK Biometrics Commissioner was established under the *Protection of Freedoms Act 2012* (UK) and is to regulate the use of biometric information and provide a degree of protection from disproportionate law enforcement action[16]. It has statutory powers that include oversight of the retention of biometric information by deciding on applications made by police to retain biometric information, as well as reporting to the Home Secretary about these functions or other matters considered appropriate. The House of Commons Science and Technology Committee has recommended that the statutory responsibilities of the Biometrics Commissioner 'be extended to cover, at a minimum, the police use and retention of facial images'[17].

We believe such an approach should be examined in Australia to improve the regulation of biometric information, not just by law enforcement, but by all government agencies, businesses and the private sector, given the increasing importance of this information in securing personal data, financial and business accounts, access to buildings and infrastructure. This function could be integrated into an existing agency, such as the OAIC, or within a new agency.

Recommendation 2: The government should introduce a biometrics commissioner to regulate the storage and use of Australians' biometric information as it becomes a primary form of identification in the online environment. Ideally, this would take the form of a new statutory authority, but it could also be incorporated within the OAIC, provided sufficient resources were allocated.

While a great deal of further work would need to be undertaken in order to assess the benefits and costs of the general approach outlined here in relation to on-line business transactions and biometrics, and how the particular suggestions would work in practice, a proactive approach of this type would go some way to addressing the negative externalities and information asymmetries referred to in the *Strengthening Australia's Cyber Security* discussion paper, that result from this information being controlled by the private sector. We recommend that such an approach should be examined further and considered in other contexts.

[16] *Protection of Freedoms Act 2012* (UK) c 9, s 20.
[17] House of Commons Science and Technology Committee, Parliament of the United Kingdom, *Current and Future Uses of Biometric Data and Technologies* (2015) 34.