15 December 2023

Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600
Submission via web:
https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/LECybercrime47

Inquiry into the capability of law enforcement to respond to cybercrime

About us

The **UNSW Institute for Cyber Security** ('IFCYBER') has the mission to apply multi-disciplinary and cross-faculty research and teaching partnerships to address sovereign interests and Cyber Security socio-technical problems. IFCYBER is a large conglomerate of 140 experts in cyber security across each of our faculties. Unique to UNSW is our understanding that cyber security is multidisciplinary. We are interested in the human, organisational, social, economic, legal, and technical aspects of cyber security. Our aim is to consider 'real-world problems' and deliver 'real-world impact' – in Australia and globally.

The **UNSW Allens Hub for Technology, Law and Innovation** ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

About this Submission

We are grateful for the invitation to make a submission to the Parliamentary Joint Committee. Our submission reflects our views as researchers; they are not an institutional position. We focus on areas related to our research. This submission can be made public.

The opportunities and challenges of the existing legislative framework in supporting law enforcement to investigate and act upon instances of cybercrime

We would like to see demonstrated, a holistic understanding of the role that different parts of the law play in making Australia a cyber-secure nation. This includes law enforcement powers but is not limited to them. It is critical that consideration of this question is not separated from but is part of

Australia's broader cyber security strategy and related law reform. We made a similar point in our submission on the Cyber Security strategy itself – our comments below are adapted from there.

The policy agenda for cyber security is driven by an ever wider and evolving list of threats and harms, from data breaches to cybercrime to foreign interference to cyber warfare. When cyber security incidents occur in Australia and elsewhere, they enliven multiple legal and regulatory frameworks, and impact civil society, the economy, and the national interest. For example, the Optus Data breach enlivened, inter alia, the *Telecommunications Act 1997* (Cth) licensing regime,[1] privacy laws, director's duties,[2] financial reporting regulation,[3] and cybercrime.[4] Overlapping and fragmented delegations of power, authority and jurisdiction came into sharp focus during the breach, with multiple regulators acting in response, including the Australian Information Commissioner,[5] the Australian Communications and Media Authority,[6] and the Australian Federal Police.[7] AustLII's Cyber Law Mapping Project and ANU's Tech Policy Atlas illustrates some of the complexity here.[8]

While the complexity and connectivity of the existing legal and policy framework presents Australian governments at Federal, State and Territory level with multidimensional overlapping problems, it need not be seen as an insurmountable problem. In a cyber security context, law operates offensively, defensively, and structurally, shaping frameworks, authority, delegations, obligations, and behaviour in multiple contexts, from civilian and defence contexts to social, political, and economic contexts. Law operates in sector-specific and cross-sectoral regulatory contexts too, meaning that legal fields, sectors of the economy and regulation overlap, yet also operate independently in distinct jurisdiction and subject matter domains. The existing overlap and fragmentation are not unusual being caused, in part, by Australia's federal structure and, in part, by the nature of cyber security itself.

---

[1] See, eg, Telecommunications (Carrier Licence Conditions—Security Information) Declaration 2022: <https://www.legislation.gov.au/Details/F2022L00958> and Telecommunications (Carriage Service Provider—Security Information) <https://www.legislation.gov.au/Details/F2022L00959>

[2] See, eg, a cyber security breach may enliven liability for directors under Section 180 of the *Corporations Act 2001* (Cth).

[3] See, eg, AUSTRAC, *Reporting obligations following personal data breaches* (Web Page) <https://www.austrac.gov.au/optus-data-breach-working-our-reporting-entities>.

[4] See, eg, Australian Federal Police, *Operation Guardian expands to combat further cybercrime* (Web Page) <https://www.afp.gov.au/news-media/media-releases/operation-guardian-expands-combat-further-cybercrime>.

[5] Office of the Australian Information Commissioner, OAIC opens investigation into Optus data breach (Press Release, 11 October 2022) <https://www.oaic.gov.au/newsroom/oaic-opens-investigation-into-optus-over-data-breach>.

[6] Australian Communications and Media Authority, 'ACMA investigation into Optus Data Breach' (Press release, 11 October 2022) https://www.acma.gov.au/articles/2022-10/acma-investigation-optus-data-breach.

[7] Australian Federal Police, 'Operation Guardian expands to combat further cybercrime' (Press Release, 28 March 2023) <https://www.afp.gov.au/news-media/media-releases/operation-guardian-expands-combat-further-cybercrime>.

[8] Tools such as Austlii's Cyber Law Map and ANU's Tech Policy Atlas are useful starting points for understanding the shape of the current legal and regulatory landscape.

Improving understanding of the different roles that law plays will assist in creating a sense of *'shared regulatory space'*,[9] which, rather than seeing overlap, fragmentation, and inconsistency in law and policy frameworks as a problem, will encourage, as Freeman and Rossi argue, a focus on the interplay between departments' and agencies' delegations, jurisdiction and subject matter expertise; on areas where agencies and departments work at cross-purposes; on ways to capitalise on their unique strengths; and ensure transparency and accountability frameworks are operating appropriately.[10]

To enhance coordination, cooperation, and collaboration in cyber security's 'shared regulatory space', we recommend:

- Clarity around intragovernmental and intergovernmental coordination and cooperation for cyber security;
- Clarity around delegations of power;
- Consider *enhanced coordination tools*, such as the creation of a 'Cyber-Reg' for sector-specific and cross-sectoral regulators with jurisdiction, delegation, discretion, or authority over cyber security.

An example: The Cyber Socket proposal

One example where law can point in different directions is the interaction between computer crime laws and vulnerability disclosure programs. This links to a proposal we have worked on with the NSW government, the idea of a 'socket' for vulnerability disclosure schemes within computer crime laws. Currently, computer offences are dealt with federally in the Criminal Code and in equivalent state/territory laws. Ideally, all would be amended as per this proposal since the problem is only resolved if security researchers are protected from prosecution nationally (given that networks cross borders).

Computer offences include offences that are unrelated to broader criminal conduct (e.g. Criminal Code, Section 478.1). In these cases, the crime could be committed where a person believes they are participating in a vulnerability disclosure program, but their acts are not, in fact, 'authorised' under the terms of that program. This can be the result of poor drafting or innocent misinterpretation.

To give an example of the problem, consider the current intersection of the law and one organisation's program (National Australia Bank (NAB)). NAB's website states 'NAB does not condone malicious or illegal behaviour in the identification and reporting of security vulnerabilities.' It is not clear how this statement intersects with illegality in the Criminal Code – is a person participating in NAB's program required to act within the law (eg not access restricted data held in a computer) as a condition of participation or does participation mean that the conduct is not illegal in

[9] Freeman and Rossi describe 'shared regulatory space', arguing that while agency coordination is one of the central challenges of modern governance, the nuanced concept of 'shared regulatory space' enables a discussion of coordination tools, practices and techniques that can improve the overall quality of decision making 'by introducing multiple perspectives and specialised knowledge and structuring opportunities for agencies to test their information and ideas': ody Freeman and Jim Rossi, 'Agency Coordination in Shared Regulatory Space' (2012) 125(5) Harvard Law Review 1131, 1136, 1210.
[10] Ibid.

the first place (because access is not unauthorised)? Further, what is the consequence when a person is registered for the program but misinterprets one of the scope statements? Even where such questions can be answered, people looking to participate in such programs may be nervous about criminal consequences (and lawyers, where they can be afforded and are consulted, may be justifiably cautious given the criminal consequences).

The proposal is to amend the computer crimes legislation to make it clear that those participating in good faith in a vulnerability disclosure program are not guilty of an offence. The laws can be amended to act as a 'socket' into which vulnerability disclosure programs can 'plug in', protecting participants from accidental criminal consequences.

Drafting the changes would be for legislative drafting offices (and different in each jurisdiction), but broadly what could be done is:

- **Define** 'vulnerability disclosure program' – this could be done through a general definition, possibly in conjunction with an 'opt in' where a registry is kept of such programs for the purposes of computer offence laws. One advantage of an 'opt in' system is the creation of a register of programs in Australia, which might be useful to the security community.
    - Ethical hacking is now also being done through AI/algorithms (e.g., Cybersecurity Cooperative Research Centre's Smart Airport project) rather than manually by human individuals. This should be included in the definition of 'vulnerability disclosure program'.
    - Currently, 'ethical hacking' activities are typically governed by standards developed in an ad hoc manner by private agreements (between companies and 'ethical hackers'), as well as by industry norms.[11] These standards ensure respect for business-oriented values (such as the protection of the client companies from harm) rather than societal and ethical values more broadly defined.[12] If a general definition of "vulnerability disclosure program" is made, this could lead to standardising and unifying ethical hacking agreements and industry norms. Given that this proposal promotes the greater social value of encouraging security research, it may be appropriate to emphasise this social value in the definition.
    - If creating an opt-in, conditions could be put on that requiring organisations opting in to agree to meet certain standards on visibility, responsiveness (including transparent timelines), clarity about rewards (recognition or monetary), agreement to make vulnerabilities public after a reasonable time etc.
    - One issue to be resolved relates to scope – Is this only for reporting to Australian companies or also to foreign companies (which raises national security issues)?

[11] See, eg, Code of Ethics for Ethical Hackers Certified by US-based organization EC-Council (International Council of Electronic Commerce Consultants) <https://www.eccouncil.org/code-of-ethics/>
[12] Jaquet-Chiffele, David-Olivier, and Michele Loi, 'Ethical and Unethical Hacking' in Markus Christen, Bert Gordijn, and Michele Loi Cham (eds.) *The Ethics of Cybersecurity*, (2020, Springer) 179–204.

- **Define** 'good faith participation in a vulnerability disclosure program' (or similar words) if that person has met any registration requirements for the vulnerability disclosure program and acted:
    - in good faith for the purposes of testing, investigating and promptly reporting a security flaw or vulnerability, in the reasonable belief that their actions were within the terms of a vulnerability disclosure program;
    - without intending to or threatening to cause harm to persons, property, or systems.

- **Choose** a mechanism that protects those participating in good faith in a vulnerability disclosure program from prosecution:
    - Option 1: Specify in definitions that conduct that is good faith participation in a vulnerability disclosure program is taken to be authorised.
    - Option 2: Create a defence to relevant offences where the conduct that would otherwise constitute the offence is within the definition of "good faith participation in a vulnerability disclosure program".

There are other legislative frameworks that provide a level of protection/immunity for those engaging in authorised activities, including testing systems and equipment and technical assistance for authorised activities. These include:

- *Telecommunications (Interception and Access) Act 1979* (Cth) s 6AAA
- *Telecommunications Act 1997 (Cth)* s 279; Pt 15 Dvs 2, 8
- *Surveillance Devices Act 2004* (Cth) (SDA) s 65A.

The example not only provides a useful law reform but illustrates the benefits of coordination across different legal domains. Incentivising vulnerability disclosure schemes also needs to consider perceived legal obstacles such as computer crime laws. Going back to the Committee's question, it is an example where limiting the scope of computer crimes (and thus the involvement of law enforcement) can enhance cyber security overall.

Prevention and education approaches and strategies to reduce the prevalence of victimisation through cybercrime

Cyber security – not the deep technical knowledge but the awareness of threats and how to take measures to avoid or mitigate risks – is now essential knowledge for everyone. This applies both from an individual (citizen/consumer) perspective and an organisational perspective (particularly for SMEs).

For individuals, we need to continue the efforts to include cyber awareness and skills in schools. This can and should be accompanied by public education campaigns, as well as encouraging school children to educate their parents, grandparents, and other relatives as part of their "homework".

Improving cyber governance and practices within organisations will require people working in a range of roles to have a range of skills. For example, those seeking careers as managers or entrepreneurs will need skills in understanding governance obligations and cyber risk for their context and building a strategy to meet legal requirements and manage risk. That strategy might

include employees or external service providers, but they will still need to ask the right questions. Organisations can benefit from more people being able to engage in "security thinking" and how to adopt an "attacker mindset" to identify vulnerabilities (not only technical but also human). Such education can be done through schools, relevant university programs (beyond Engineering) and government information and guidance for SMEs.

Yours sincerely,

Lyria Bennett Moses

Sanjay Jha