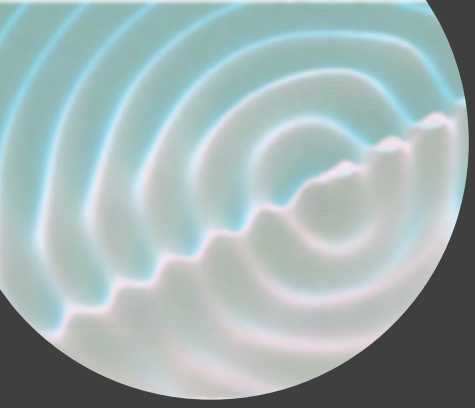
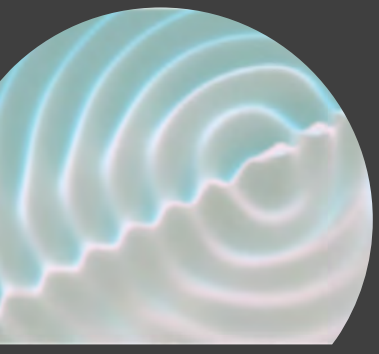
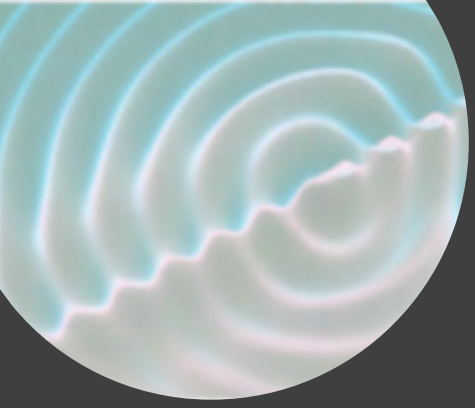
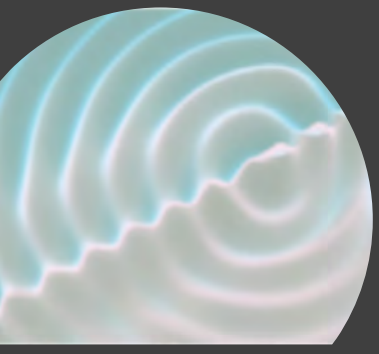




Submission

Department of Home Affairs
Discussion Paper:
Strengthening Australia's cyber security regulations and incentives





About ACLI

The Australasian Cyber Law Institute is a professional association for specialists passionate about the effective governance of cyberspace.

Membership is for professionals and organisations with a stake in advancing the development and professional practice of cyber law.

Copyright and Moral Rights

Contents

Acknowledgements

- Working Group:
  - Chair: EJ Wise.
  - Co-Chair: Emma Watson.
  - Secretary: Nick Dyson.
- Co-Author and Designer: Carol Grimshaw
- Co-Author: David Bowles, Ethics Special Counsel, ACLI Director and Board Member.
- ACLI's Star/Bar Rating System Author: Emma Watson.
- Editing support: Michael Hill.

Definitions

ACLI : Australasian Cyber Law Institute, 6/8 Bromham Place, Richmond Vic 3121, M: 0487 966 813. Contact chair@acli.org.au.

ACL : Australian Consumer Law.

ACSC : Australian Cyber Security Centre

ASIC : Australian Securities and Investments Commission.

ASX : Australian Stock Exchange.

Business : any firm engaged in a lawful activity in the pursuit of profit and may include government corporations.

Consumer : any individual over the age of 16 engaged in the retail purchase of products from the Australian and/or global market.

Cyber secure : having taken measures to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

Data : information in digital form that can be transmitted or processed or stored.

Data holder : and can include Business, Small business, Medium business, Large and Larger Business, Retail Business, NGOs and Government entities.

Definitions

EWOWC : Electronic Wills and Online Witnessing Committee, the inaugural Committee of the ACLI.

Large and **larger business** : any firm engaged in a lawful activity for the pursuit of profit with an annual turnover between exceeding $100 million.

Medium business : any firm engaged in a lawful activity for the pursuit of profit with an annual turnover between $50 million and $100 million.

Non-government organisation or **NGO** : any industry body, think tank, industrial organisation.

Personal information : identification data, financial data, health data, government records, legal records, intimate partner records, and all images connected to each category of personal information.

OAIC : Office of the Australian Information Commissioner.

Retail business : any business that interacts with a member of the public with the intent of selling its wares.

Small business : any firm or individual sole trader engaged in a lawful activity for the pursuit of profit with an annual turnover between $0 to $50 million.

SME : small to medium enterprise currently operating in Australia with an annual turnover of under $50 million.

Submission Structure

ACLI's Submission is arranged in 11 chapters which correspond to the 11 chapters in the Department of Home Affairs' Discussion Paper: *Strengthening Australia's cyber security regulations and incentives.*

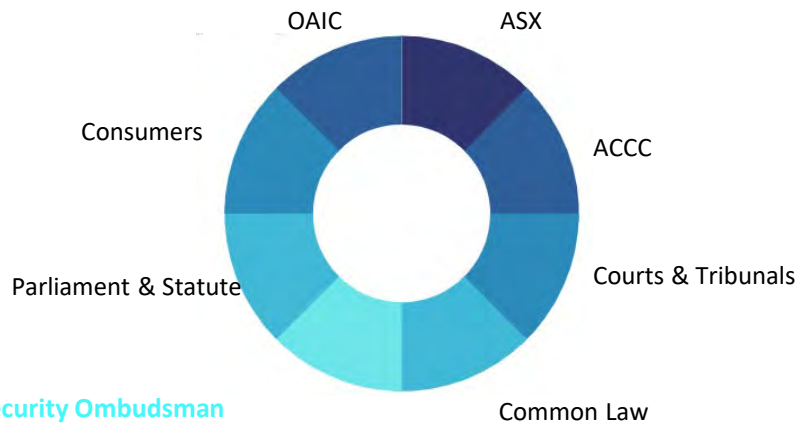
Where the discussion and recommendations relate specifically to a question raised in *Appendix A: List of discussion questions* of the Discussion Paper, this is indicated [*Appendix A: q 9*].

Chapter 1

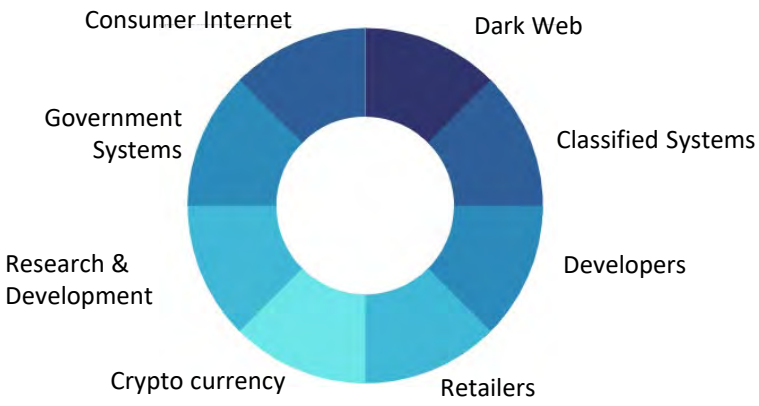
The Ecosystem: Context of the Problem

The Ecosystem

Legal Environs

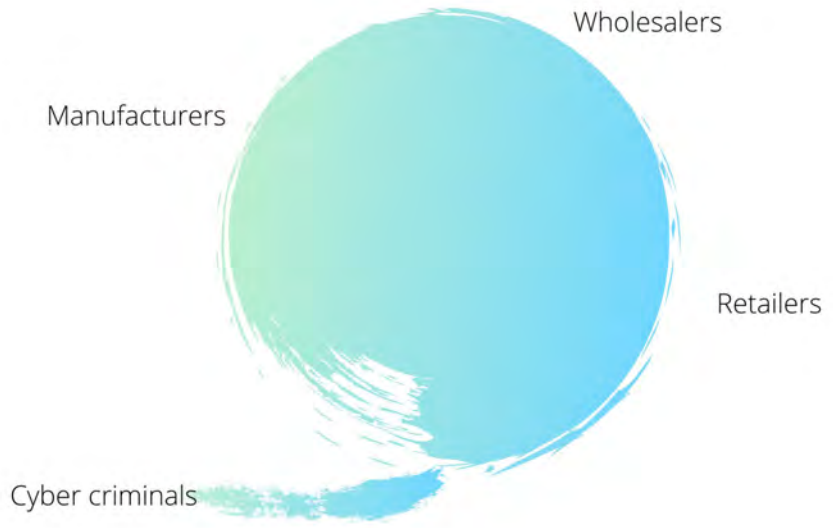


Tech Environs



Business to Business and Business to Consumer

Who's who in the B2C and B2B world?



Chapter 2

Why Should Government Intervene?

Why Should Government Intervene?

The free market does not currently reward ethical treatment of other people's information

- Australia's cyber security regulatory and legal framework does not adequately protect consumers.
- There is currently no incentive for a business to minimize the amount of high value Personal Information it holds, loss of which may damage others. There is no incentive to limit dissemination nor ensure the attack surface is reduced.
- Current arrangements provide little market advantage or incentive for SME's to invest in cybersecurity. Smaller enterprises or start-ups that choose not to do so may enjoy a short term price advantage.
- A consistent national policy is essential.

Small Business Sector is especially vulnerable and needs protection and support

- Small businesses comprise an extensive variety of human endeavour ranging from a sole trader plumber to a medical clinic with several general practitioners and staff.
- The cyber security risks within each small business and subject matter sector differs significantly depending on the type and amount of information it gathers, processes, retains and destroys. These are not necessarily caught by the existing privacy regime, where small business is often the least informed about cyber security or their duties to third parties.
- The various types of small business should be categorised according to the 'information risk profile' they represent i.e. the type and quantity of information they process and hold.
- Lawful access to personal information can be for multiple lawful reasons by various participants in one transaction: the gatherer, the storer, the administrator, and the destroyer of the information. Each of these may be strangers to the owner of the personal information making cyber security ever more important from a policy level. Moreover, the data held through each phase of a transaction may be held in different systems, locations and jurisdictions than what is known or disclosed to the owner of the personal information.

Why Should Government Intervene?

Not all small enterprises are the same. Turnover is not an adequate factor to determine risk.

- Small businesses comprise an extensive variety of human endeavour ranging from a sole trader plumber to a medical clinic with several general practitioners and staff.
- The cyber security risks within each small business and subject matter sector differs significantly depending on the type and amount of information it gathers, processes, retains and destroys. These are not necessarily caught by the existing privacy regime which adopts the very crude measure of business turnover to determine whether regulation applies.
- The various types of small business should be categorised according to the 'information risk profile' they represent i.e. the type and quantity of information they process and hold.

Those most affected by information loss often have no ability to influence the risk.

- Lawful access to personal information can be for multiple reasons by various participants in one transaction: the gatherer, the storer, the administrator, and the destroyer of the information.
- Each of these may be strangers to the 'owner' of the personal information. The person with the most to lose from disclosure may have no contractual relationship with the information custodian and no economic power to influence the level of care.
- Moreover, the data held through each phase of a transaction may be held in different systems, locations and jurisdictions than what is known or disclosed to the owner of the personal information
- This makes regulatory intervention particularly important.

Why Should Government Intervene?

Small Business Sector – barriers to best practice [*Appendix 1: q1*]

- Some of the factors preventing Australian Small Business from adopting cyber security best practice include:
  - Australia has lacked clearly stated cyber measures as the 'recommended minimum' for all small businesses.
  - There has been little market advantage or incentive for small to medium enterprises to invest in cyber security. If anything, the reverse is true. It is cheaper to claim that 'we take security seriously' than do anything about it.
  - Australia lacks a coherent program of information/education specifically targeting small businesses that makes it clear that a business with anything less than a 'recommended' minimum standard of cyber security is putting its clients at risk, and that not acting to address the situation could potentially be considered negligent.
- The general public needs to be informed and educated that doing business with a Small Business that chooses not to satisfy a 'recommended' minimum standard of cyber security puts the consumer at risk. This education will allow a consumer to make better choices for their cyber safety.
- A simple example on a Business to Business level is the application for and provision of trade credit. This happens daily between trades, trades and service sectors, sole traders and partnerships, single director/secretary companies and trading trusts.
- Each side of the transaction – creditor and putative debtor – exchanges substantial commercial and/or Personal Information. Formerly delivered by a facsimile machine, electronic/digital communication and the resulting cyber security risks attach to each applicant. Many would not consider their applications to be an information, legal, identity, or financial risk.
- Unless regulated by the Privacy Act, in most cases the recipient currently has no legal obligation to apply even basic cybersecurity measures.

Chapter 3

Current Regulatory Framework

The Current Regulatory System

Limitations of the current system [*Appendix A: q3*]

- Regrettably, the current system lacks cohesion and sufficient incentives to business to protect consumers of all forms from cyber breaches and criminals.
- Consumers, especially non-business consumers, are not attuned to the cyber-risk involved in their purchases, particularly of domestic smart devices.
- In this way, the 1960s era fears that our televisions would monitor our private lives have a more factual basis than ever before, while users are more trusting and reliant on smart devices.
- There are few practical avenues for an affected consumer or small business to seek redress, compounded by the lack of real world regulatory consequences.

Consumers and those who have lost critical data have few avenues of redress

- Larger enterprises can treat small compensation payments and modest fines as a cost of doing business. They are thus undeterred from permitting sale and use of products with high cyber security risk.
- The incentives to profiteering from cyber security breaches include the inability of individuals or groups to bring tortious claims for adjudication through small claims jurisdictions, the Courts and through regulators.
- The lack of a specific jurisdiction for these claims is problematic as is the inability of real world consequences being sheeted home to business through the ASIC, the ACCC and the ASX.
- Causation as it is understood in law is a barrier to the adjudication of disputes because it is the method through which responsibility is apportioned. Better systems need to be developed.

Chapter 4

Governance Standards for Large Business

Governance Standards for Large Business

- Larger businesses have a positive obligation to protect certain classes of information, and their directors have a duty pursuant to ss.299-300 of the *Corporations Act* 2001 (Cth) to consider and address cyber resilience. Some sectors have specific regulation (cf, CPS-234 for APRA regulated entities) but there is no consistent methodology applied across the private sector.
- Information loss tends to impact business' reputation for a limited period and that is a limited disincentive for business to change. The consumers who may be effected are only known through media reports and referenced as numbers. Compliance and remedies for cyber security seem to be back of mind for Large Business.

Recommendations [*Appendix A: q5*]

- The back-of-mind approach can be resolved by annual compliance reporting to ASIC by all corporations when filing annual returns.
- Each annual report can be one page longer to identify the cyber security measures taken to ensure customer/public security proportionate to means and station. Individual directors and Chief Information Officers can be required to attest to the veracity of the report content.
- Annual reports should also identify the preceding year's cyber security failures and disclose those failures to whichever government agency adopts a cyber security monitoring function. This can be a separate arm of the Ombudsman we propose, the **Cyber Security Ombudsman**.
- Failure to comply with mandated cyber security minimums for Large Business should result in fines which becomes a fact for formal public disclosure on the freely accessible ASIC Register.
- The relevant cyber security agency – the **Cyber Security Ombudsman** - should be empowered to investigate Large Business breaches for failure, deceit and tardy actions taken by Large Business.

Governance Standards for Large Business

- Publicly listed entities should be required to notify the ASX and issue a ASX press release reporting on cyber security failures and redress steps taken.
- Wherever a Large Business is a recidivist, the corporation should be exposed to delisting. Equally, their Directors and CIOs should be prevented from using the safe harbour provisions of the *Corporations Act* 2001 (Cth).
- Fines and related interest on the fines to Large Business should be channelled into a damages' pool. Recidivist Directors and/or CIOs should face personal liability for the damage caused to consumers.
- The damages' pool should pay for:
  - public education about business responsibilities for cyber security
  - a new federal body, with an investigations and dispute resolution focus – the **Cyber Security Ombudsman** - that vets small claims where the claim is under $10,000 and does not include personal injury or defamation.
- Lawyers should only be permitted to represent claimants for claims under $10,000 with approval from the **Cyber Security Ombudsman**.
- Claims exceeding the $10,000 threshold should be certified for recovery through the existing Court system.
- We also recommend the GDPR approach of requiring a 4% fee from Large Business to support a scheme for compliance. Those funds will assist in public education and funding the **Cyber Security Ombudsman**.

Organisational maturity and cybersecurity – the challenge

- There is a 'catch-22' problem in cyber governance. Organisations with low governance maturity typically regard cybersecurity as a technical problem, and do not understand the multi-faceted nature of the organisational response that is required.
- The governance improvements a business needs are often not appreciated or embraced until that governance is in place.
- Information security projects often do not improve system functionality. In fact, they can make life more difficult.

Governance Standards for Large Business

Organisational maturity and cybersecurity – the challenge

- An expensive project requiring 'interference' across multiple facets of an organisation without any tangible deliverables other than mitigating a risk that is poorly understood is not an attractive proposition. In many instances the response is delegation of responsibility to the IT department.
- Information security driven primarily as a technical function is significantly less effective. Policy, training and cultural issues are an essential part of the maturity journey, and a technical department will have significant difficulty co-ordinating these. Policy applied from the IT department alone tends to be generic, not well suited to the business workflows and poorly understood or implemented by the coalface work force.
- Expert consultants dealing with the IT department are often preaching to the choir, and information to the c-suite can be seen as sales for their consultancy and monitoring services.

Recommendations

Mandatory governance training [*Appendix A: q5*].

- All Privacy Act regulated entities should have at least one board member or senior executive with a cyber-governance qualification.
- This qualification should not be difficult or lengthy – a few weeks commitment would be sufficient.
- The objective is to improve cyber risk governance, not to create a hands-on expert. The best analogy is occupational health & safety improvement which is familiar to many organisations. As there is no statutory authority or compulsory insurer to drive risk management, the regulatory framework should ensure that there is at least a senior voice within the business that has that understanding.

Governance Standards for Large Business

Recommendations

Assist directors to understand and articulate cyber risk [*Appendix A: q6*].

- Appropriate management tools to assist directors to determine the risk across the organization and articulate this to their peers would be a significant benefit.

Voluntary governance training [*Appendix A: q7*].

- Owners / managers of smaller enterprises should be provided free or subsidised risk training. The objective should be to assist them to understand the cyber risk in the context of their own industry. Peak bodies would be ideal partners to deliver this training.

Chapter 5

Minimum Standards for Personal Information

Minimum Standards for Personal Information

Where does the current approach fail?

- Vast swathes of critically confidential personal information may be held by business, government and NGOs of all kinds, with little regulatory oversight.
- While the nature of the information held is relevant to considering 'reasonable steps' under Australian Privacy Principle 11[1], this is not explicit and does not adequately differentiate between casual information held in some circumstances as opposed to the high value data held in others.
- Examples across industry sectors are illustrative of the challenges faced by everyday consumers.

Residential accommodation example:

- A standard application for rental accommodation is very invasive. A prospective tenant may be required to provide copies of passport and driver's license, banking and income details, former addresses, employment and asset statements.
- This information must be emailed, or uploaded onto a third party app without any notice of terms and conditions, or undertakings regarding information security.
- Tenants have little scope to object to the information sought nor negotiate how it will be held.
- In many instances, the managing agent will be a franchisee with a turnover under the Privacy Act threshold. In those circumstances, APP 11 will not apply.

[1] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/?start=0&tags=106

Minimum Standards for Personal Information

Recommendations

- ACLI recommends the ACSC Essential Eight as a mandatory minimum standard and in addition the Top 4 of the ACSC Strategies to Mitigate Cyber Security Incidents as a mandated requirement.
- Consumers should have a way to assess the relative security of products and devices that collect or store their personal information, or which connect their home digital environment to the internet.
- A star rating system could cover such issues as:
    - cost effectiveness;
    - cyber safety;
    - environmental harm;
    - energy use;
    - dis/ability friendliness.
- Certification to be issued by the same government agency who issues fines, the **Cyber Security Ombudsman**.
- We agree to the implementation of a cyber security code, administered by a **Cyber Security Ombudsman**, however it should have wide application and not be restricted to entities regulated by the *Privacy Act* 1998 (Cth).
- Entity turnover should not be the precondition to compliance. All entities holding personal information should meet the Minimum Standards Code.
- A further classification of Personal Information should be added to the *Privacy Act* 1998 (Cth): 'high value personal information'. Regulations specific to this classification would then be possible, enabling more targeted and nuanced protections [Appendix A: q10].

Minimum Standards for Personal Information

Recommendations

- A possible definition of 'high value personal information' is:

  High Value Personal Information includes:

  - Electronic and digital copies of identification documents
  - Medical and health information
  - Legal information
  - Financial records, including transaction history and account details, credit card numbers, cryptocurrency accounts, share records etc.
  - Information which may place an individual at risk of harm if released.
  - Information which is likely to cause high levels of distress or economic loss if released.
  - Information which would reasonably facilitate identity theft or crime.
  - High volumes of Personal Information that does not meet the other criteria of this definition.

- We consider that the best starting point technical controls as a mandatory code would use the UK's Cyber Essentials for smaller entities, and the Essential 8 for larger ones.
- Additional risk mitigation dimensions would also be required:
  - Policy adoption in such areas as access credentials, encryption, shadow IT, and appropriate locations of sensitive data;
  - Physical security measures;
  - Pre-recruitment checks;
  - Induction and refresher training.
- Inherently, a generic code will struggle to be equally useful across all sectors of the economy. What is appropriate for, say, a migration agent would be overkill for a painting company.
- *Industries should be given scope to negotiate a more appropriate code* through their peak bodies or member associations. To avoid a race to the bottom, the approval agency – the **Cyber Security Ombudsman** - should adopt a 'no consumer detriment' test.

Minimum Standards for Personal Information

What effective technical controls should be included?

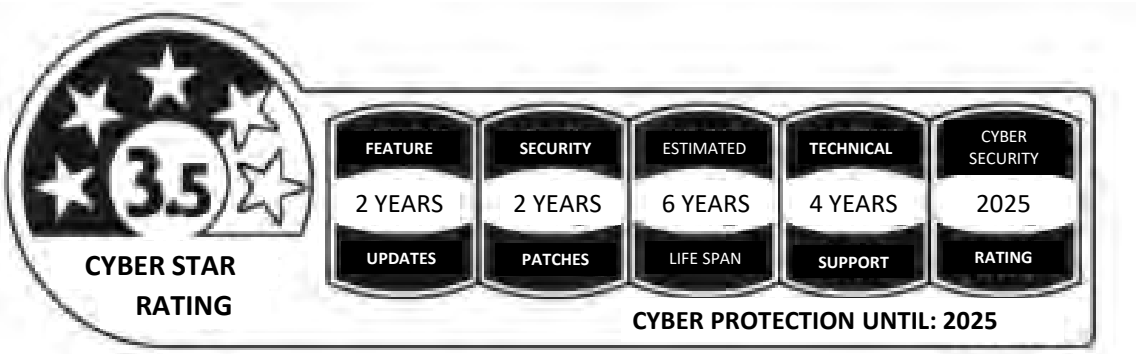
- The best starting point for technical controls as a mandatory code would use the UK's Cyber Essentials for smaller entities, and the Essential 8 for larger ones.
- Additional risk mitigation dimensions would also be required:
  - Policy adoption in such areas as access credentials, encryption, shadow IT, and appropriate locations of sensitive data;
  - Physical security measures;
  - Pre-recruitment checks;
  - Induction and refresher training.
- Inherently, a generic code will struggle to be equally useful across all sectors of the economy. What is appropriate for, say, a migration agent would be overkill for a painting company.
- Industries should be given scope to negotiate a more appropriate code through their peak bodies or member associations. To avoid a race to the bottom, the approval agency – the **Cyber Security Ombudsman** - should adopt a 'no consumer detriment' test.

Chapter 6

Standards for Smart Devices

Standards for Smart Devices

ACLI's Proposed Star/Bar rating label:



What the label tells consumers

- **Feature Updates**:
  - The lifespan for updates being provided to enhance and expand the features and capabilities of the product for example operating system updates such as iPhone IOS13 to IOS14.
- **Security Patches:**
  - The lifespan for updates being provided that fix vulnerabilities in existing operating systems and does not include any additional features or functionality.
- **Estimated Life Span:**
  - how long the manufacturer expects the product to last and intends to supply replacement parts. For example, Apple has a 7 year lifecycle from date of model commencement.
- **Technical Support:**
  - how long the manufacture guarantees technical assistance with the product either online or in person.

Standards for Smart Devices

What the label tells consumers

- **Cyber Security Rating:**
  - ACLI prefers Singapore's cyber security rating model due to its simplicity which makes it consumer friendly in comparison to the UK Model.
  - rated by approved third parties against a standard.
- ACLI's Star/Bar system demonstrates what may be accomplished for the marketplace to convey:
  - cost effectiveness of the product
  - cyber safety of the product
  - environmental harm including the cost to produce the product
  - energy use and cost to the consumer and small business in installing and using the product
  - dis/ability friendliness to ensure cyber security does not become an area of discrimination
  - Feature updates
  - Security patches
  - Estimated life span
  - Cyber security rating
  - Technical support

Standards for Smart Devices

What the label tells consumers

- The dates involved should reflect the contractual sunset between purchaser/vendor for each item in the rating system.
- The system is readily understandable in the marketplace by consumers, manufacturers and retailers.
- Certification of each standard should be issued by the same government agency – the **Cyber Security Ombudsman** - who is empowered to issue fines for non-compliance.

Chapter 7

Labelling for Smart Devices

Labelling for Smart Devices

- We recommend our Chapter 6 Star/Bar rating label design for a Smart Device label.
- Protections for consumers and small business should be focussed at providing clear information that is easily digested.
- Given the recognition of the system across Australia's white goods and vehicle sectors of a star rating system, ACLI recommends the design and implementation of a similar system for smart devices.
- The labels should have a print date to allow for product dating, similar to those used by Apple Inc.
- The star rating system certification should be issued by the same government agency who issues fines to medium and large business who fail to meet minimum privacy and cyber security standards referenced in Chapter 5 of these submissions.

Chapter 8

Responsible Disclosure Policies

Responsible Disclosure Policies

- When created, the **Cyber Security Ombudsman** will be empowered to issue certificates after matters are arbitrated. Until that time, the OAIC should be allocated that power and the resources to properly administer a new division to assist with disclosure.
- Power to issue certificates for matters with damages exceeding $10K.
- We recommend the ASIC, ASX and OAIC disclosure notices be legislated, as above.
- Privacy Principles apply to business above $3M which is annually annexed. This is a high threshold for everyday retail business, often capturing identifying details from their consumers. We recommend the threshold not be solely based on the income levels of business as this will omit remedies for many consumers.
- Vendors should be required to pay cyber security bounties imposed on consumers.
- Cyber security insurance should be a standard part of creating a business and purchased within 7 days of establishment.
- Disclosure needs to be mandated once the vulnerability is secured. That disclosure includes to those who are immediately impacted and second-tier victims otherwise mentioned in this submission.
- Insurance companies tend to limit an insured's disclosure to reduce their exposure. This standard needs to be altered to ensure the insurer does not impede protection of individual privacy and promotion of cyber security.
- An incentive for insurers and insured would be to have a positive health check from the **Cyber Security Ombudsman**. Initially, a tied grant could operate to achieve nationwide cyber security through the insurance industry.

Chapter 9

Health Checks for Small Business

Health Checks for Small Business

- Government sub-agency should be established within Federal Business Portfolio to assist small business comply with mandated standards. This educative function could be an arm of the Cyber Security Ombudsman.
- We recommend an initial lead-in period where non-compliance by Small Business is not penalised. This should not be extended to Large Business because it is well resourced and has dedicated teams for cyber security and staff training.
- For Small Business, these health checks could act as a government styled help desk for cyber/tech training and addressing emerging issues, because small business lacks the resources for implementing new policies.
- The lead-in time could also provide tied grants to the cyber security industry and tax rebates to businesses, NGOs and consumers.
- Investigators from the private cyber security industry and then – when created – the **Cyber Security Ombudsman** could be invited to assist Small Business by identifying gaps and recommending change to be implemented. Much like the best audits, the investigation session would be a knowledge exchange to assist Small Business to avoid repeat mistakes.
- Small Business could take annual classes and submit their reports for the ASIC and/or ASX to ensure they are cyber healthy. This will address the current low levels of cyber security literacy which impacts any self-assessment regime.
- Wherever falsified health checks are discovered through the disclosure and/or audit phase, penalties must be imposed on the business. Recidivists should face criminal penalties.
- The requirement for cyber health checks could be integral to cyber insurance.

Chapter 10

Clear Legal Remedies for Consumers

Clear Legal Remedies

- The discussion paper identifies the numerous challenges in establishing clear legal remedies for consumers. These include determining what went wrong and access to justice.
- Without appropriate measures these limitations could soften the accountability and deterrence impact of legal remedies.

Recommendations:

- Reverse the onus of proof. A Business defendant/respondent and/or its Director(s) and/or Chief Information Officer becomes responsible for *establishing that it did* maintain acceptable levels of cyber security.
- A reverse onus of proof reduces the burden on consumers after a cyber incident. This is important for many consumers who have low cyber security literacy, and also those who experience health and financial disadvantage.
- The regulatory impact of a reversed onus of proof should be minimal. Organisations that have acted with due care and diligence following the system we recommend will have documented processes clearly showing cyber security compliance. This will also be reflected in their disclosure to the ASIC, ASX and through the **Cyber Security Ombudsman** when it is created.

Actions in the Torts of Negligence and Privacy

- The relationship between consumer and vendor is well-established law: *Donoghue v. Stevenson* found the manufacturer liable for the snail contamination of the opaque bottle. Cyber security is as simple and complex to a consumer as that contamination and bottle.
- Current actions for breach of confidence are inadequate measures in the cyber security space as they require the establishment of a relationship of confidence. This means we require a different approach.
- Business should be assigned an actionable duty of care with Personal Information such that it is reasonably foreseeable that capturing, holding, storing, manipulating, administering, using, selling, and/or destroying data are all activities that – if improperly managed – may give rise to economic, psychological and reputational loss for which objectively identifiable failures by Business ought to be compensated.
- Tortious suits should be made available below a statutory threshold where lawyers are not permitted to participate.
- Tortious, contractual and statutory suits should be permissible above mid-range Court minimum jurisdiction levels (County ($100K)/District).

Clear Legal Remedies

Actions in the Torts of Negligence and Privacy

- We recommend the creation of a new overarching entity with responsibility for educating the community, investigating claims, and settling disputes. We have referred to it so far as the **Cyber Security Ombudsman**.
- Until the **Cyber Security Ombudsman** is created and staffed, we recommend that the OAIC and/or super tribunals within states issue arbitration/authorisation certificates permitting litigation to commence (see domestic building disputes and retail lease mediations in Victoria as examples).
- Australian States and Territories lack legislation similar to the *Charter of Human Rights and Responsibilities Act* 2006 (Vic).
- The **Cyber Security Ombudsman** can draw statutory power for privacy claims on a tortious basis from jurisdiction Article 17 of the United Nations *International Covenant on Civil and Political Rights*, as ratified by Australia and introduced domestically in the *Australian Human Rights Commission Act* 1986 (Cth) Schedule 2.
- Australia has been slow in developing a substantive cause of action for breaches of individual privacy. As noted above, this is connected to the jurisprudential locus of claims being satisfied by breach of a confidential relationship.
- The following cases are the type that have been adjudicated and which the development of a statutory tort could flow given Australian common law developments:
    - *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 at [40]-[42] and [106]-[132] and [189]-[190]
    - *Grosse v Purvis* (2003) Aus Torts Reports 81-706; [2003] QDC 151
    - *Giller v Procopets* [2004] VSC 113 at [187]-[189]
    - *Kalaba v Commonwealth of Australia* [2004] FCA 763
    - *Doe v ABC* [2007] VCC 281
    - *Gee v Burger* [2009] NSWSC 149
    - *Power v Mann* [2010] VCC 1401 on unlawful video capture of private information

Clear Legal Remedies

Actions in the Tort of Privacy

- *Davis v Mann* [2010] VCC 1402 on unlawful video capture of private information
- *Wilson v Ferguson* [2015] WASC 15 where breach of confidence is pursued but cites *Lenah*, *Giller* and the UK position on privacy, and is approved in *Moran v Atrum Coal NL [No 3]* [2015] WASC 219.

- From a policy perspective, the tort should become available because of the severity of damage inflicted on victims of privacy breaches, evidenced in the case law on confidential information to date.
- The breach can result in types of loss that are not suitable merely to contractual remedies or those more commercial remedies under the *ACL*. Insofar as the *ACL* empowers super tribunals to hear claims about personal injury, it is limited in nature due to the generally limited experience of sitting members whose backgrounds may not necessarily even draw from the law nor a relevant technical specialty.
- Given the ease with which technology can spread a privacy breach, the impacts can be felt far longer and more broadly than the duration of the breach itself and thus severely limit the lives of those impacted.
- It is not merely the victim of the privacy breach who is impacted. Those proximate to the victim through familial, or other close relationships including an employer, can experience adverse effects. This reinforces the need for a system that adapts to the needs of victims while providing reliable methods for dispute resolution

Classes of Defendants/Respondents to Tortious Claims

- Directors/Chief Information Officers of manufacturers and/or retailers
- Limitation: responsible to the extent they fail to take action to ensure their products are designed against cyber crime and in accordance with the standards outlined in Chapters 5 and 6.
- While individuals decline liability for third party conduct, in law liability already exists via the doctrine of agency regardless of individual desires or any change we have proposed to law.
- Insofar as the corporate veil exists through the doctrine of separate legal entity, modern corporations law indicates the veil will be pierced when suitable.
- The business judgment rule should be refined/limited as a defence to these claims.

Clear Legal Remedies

The Forums

- While the office of the **Cyber Security Ombudsman** is being created, existing structures should be used to administer the summary jurisdiction of cyber security claims.
- Super tribunal jurisdictions should be extended under threshold:
  - Easy and low cost claims to threshold where lawyers are not permitted to participate in hearings, eg VCAT currently will not permit representation for claims under $15,000;
  - Business to Consumer;
  - Disability/cyber security intersection can also be administered in existing forums.
- Would hear breach of contract, statutory duties including the statutory tort of privacy outlined above, and negligence actions.

Why a Court/Litigation?

- Existing legal mechanisms are in place to deal with serious complaints including psychological injury and defamation. Those causes of action are not, or not adequately, addressed within the *ACL*, and the Tribunals implementing the *ACL* do not have the skill or jurisdiction to manage psychological injury or defamation claims.
- Urgent applications should be available for injunctive relief. The existing Court systems have well-developed tests and procedures for injunctive relief.
- The existing system is understood by common users (government, lawyers, civil society, business and sophisticated consumers etc).
- In particular, Supreme Courts of State and Territory jurisdictions have judge managed lists to deal specifically with technology matters – staff knowledge and court resources are well-established to serve their communities.

Clear Legal Remedies

Why a Court/Litigation?

Subject Matter	Super Tribunal - Without Lawyer	Super Tribunal – Super Tribunal – With Lawyer as of right	Intermediate Court	Superior Courts
Torts/Contract	$0 - $10,000 excluding personal injury	$10,000-$100,000 excluding personal injury	$100,000 right of appeal on point of law and fact. Inherent jurisdiction	• Appeal from intermediate Court on point of law • Inherent jurisdiction on technical, group or complex claims.
Privacy Act – Small Claims of pure economic loss	**OAIC to $10,000 damages**	**OAIC $10,000 to $100,000**	**Claims greater than $100,000 including personal injury**	**Right of Appeal on point of law from Super Tribunal for claim above $10,000** **Right of appeal on point of law or de novo from intermediate Court**
Privacy Act	OAIC	OAIC	Claims greater than $100,000	Federal Court of Australia
ACL	**$0 to $10,000 damages excluding personal injury**	**$10,000 to $100,000 excluding personal injury**	**Claims greater than $100,000**	**Right of appeal on point of law from Intermediate Court or right of appeal on point of law or mistake of fact from super tribunal for claims exceeding $10,000**
ACL	**$0 to $10,000 damages excluding personal injury**	**$10,000 to $100,000 excluding personal injury**	**Claims greater than $100,000**	**Right of appeal on point of law from Intermediate Court or right of appeal on point of law or mistake of fact from super tribunal for claims exceeding $10,000**
Corporations Act/Regulations	**Civil jurisdiction to $10,000 claim for pure economic loss against individual Director and/or Chief Information Officer**	**Civil jurisdiction $10,000 to $100,000 claim for pure economic loss against individual Director and/or Chief Information Officer**	**Federal Circuit Court of Australia or State/Territory Courts for first breaches** **Appeal to Federal Court of Australia or Supreme Courts**	**Federal Court of Australia in its inherent jurisdiction** **Supreme Courts in their inherent jurisdiction** **State/Territory Law change: Corporations matters must be heard in superior Courts**
Criminal			**Federal Circuit Court of Australia for summary matters; appeal to State/Territory Courts or Federal Court of Australia**	**Federal Court of Australia in its inherent jurisdiction** **Supreme Courts in their inherent jurisdiction**

Chapter 11

Other Issues

Cyber Crime

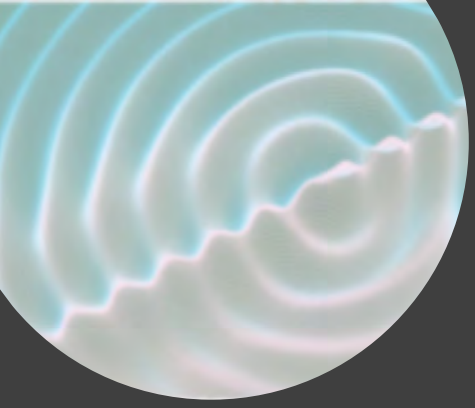
Cyber Crime

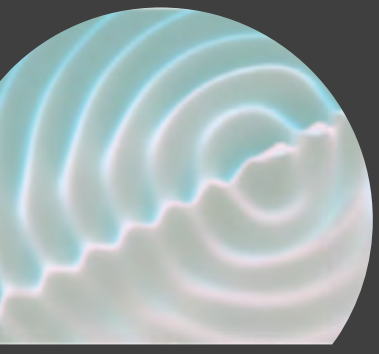
- As the final piece in the cyber security ecosystem, cyber crime plays a substantial role. Indeed, it is what necessitates the counter measures we recommend for protection of the balance of the ecosystem.
- Due to the nature of this aspect of the cyber industry, operating as is it does on the dark web and through antisocial channels, it's purpose is to evade the legal system.
- However, we recommend that criminal penalties be designed to take into account the impact the activity has on society.
- Whilst the penalties arising from Pt 10.7 of the *Criminal Code Act* 1995 (Cth) are generally sufficient, the cyber fraud and extortion chain requires numerous support services.
- Professionals who assist money laundering, smurfs and low end criminals establishing false-name bank accounts all facilitate the principal offenders.
- As these are the parts of the ecosystem most commonly within our territorial jurisdiction, resources should be devoted to ensuring an increased rate of detection. Maximum penalties should also be increased
- In particular, finance professionals who knowingly participate in or are wilfully blind to the assistance they provide to cybercriminals deserve criminal sanction.
- The appropriate penalty range should be consistent with the existing penalties for money laundering (ss. 400.3 – 400.8 of the Criminal Code), save that additional penalties based on the turnover of the professional practice should be available.

Sections of the *Criminal Code*	**400.3**	**400.4**	**400.5**	**400.6**	**400.7**	**400.8**
Money / Property Value	$1 million or more	$100,000 or more	$50,000 or more	$10,000 or more	$1,000 or more	Any value

Cyber Crime

Sections of the *Criminal Code*		**400.3**	**400.4**	**400.5**	**400.6**	**400.7**	**400.8**
Penalty	ss (2) Recklessness	12 years	10 years	7 years	5 years	2 years	6 months
	ss(3) Negligence	5 years	4 years	3 years	2 years	12 months	10 p/units





Contributors

Participant Biographies

EJ Wise

Founding Chair and Director, ACLI, Chair – Cyber Security Submission Working Group, Adjunct Professor, Faculty of Science, Engineering and Built Environment, Deakin University

Sessional Academic, Thomas More Law School, ACU,
Founding Director, National Institute of Strategic Resilience,
Member Law Institute of Victoria Technology & Innovation Section, Member Law Institute of Victoria IPIT Committee, Member Belgium Avenue Neighbourhood House Executive Committee

EJ Wise is the Principal of Wise Law Cyber Consulting, specialising in Cyber Security Law, and in her capacity as ACLI Chair has chaired this Submissions' Committee.

Before founding Wise Law, EJ's path was unique in every way.
EJ has been a practising lawyer for the last 27 years, of which 21 years were served in the Royal Australian Air Force (RAAF) as a commissioned and uniformed officer, and as advisor to the Australian and State Governments on law and policy.

EJ also served the United States Air Force in their Operations & International Law Division in Washington DC for 3 years as the RAAF's No. 462 Cyber and Information Operations Legal Officer.

EJ is an internationally recognised expert in Cyber Law, a keynote speaker and an author who has been published in various law journals and magazines on the topic of cyber law and ethics. EJ's latest project is to develop a Union for Lawyers in Victoria.

EJ has assisted in drafting laws and relevant texts and manuals in Australian, International and US jurisdictions. She has assisted in law enforcement as well as cyber operations. EJ has strong community values and gives her time to community and not for profit organisations as her contribution to a fairer, more inclusive and equitable society for everyone.

When EJ isn't leading the ACLI team or volunteering for a variety of causes, she spends time with her family and 3 cats in her inner Melbourne suburbs home.

Participant Biographies

Carol Grimshaw

LL.M. (Applied), LL.M. (LP), B. Legal Studies, Adv. Dip. Business,
Admitted to practice in Victoria and the High Court of Australia, 2010
ACLI Director and Board Member, ACLI Member, Chair, EWOWC,
Founder, 'The 'Dear Sirs' Project', Graduate Fellow, College of Law
Member, Law Institute of Victoria, Member, Ballarat Business Women, Member, Women in Insolvency Victoria, Member, Australian Women Lawyers, Member, Femeconomy, Member, Family Law Section of the Australian Law Council

Carol Grimshaw is the Principal of Grimshaw Legal and Aide Lawyers. With a career commencing in the Melbourne legal sector in 1996, Carol worked and studied simultaneously toward admission to practise while gaining further experience through volunteering at community legal centres.

Carol's keen eye for efficiency and technology resulted in her working for firms across the legal strata, and at government and semi-government organisations with a focus in dispute resolution. This experience allowed Carol to identify the many opportunities for enhancing consumer interaction with the legal system through technology.

As EWOWC Chair, Carol assisted in the creation of the Victorian legislation that makes electronic signing and witnessing a permanent possibility for all Victorians. Taking a role on the Board in early 2021 has increased Carol's contribution to the ACLI and her leadership in co-authoring this Submission, with a particular emphasis on the ecosystem and clear legal remedies that ACLI looks forward to becoming a future part of the Australian legal system.

Carol has recently moved to regional Victoria and looks forward to returning to community volunteer service. When not volunteering, Carol enjoys the natural environs, art, history, and politics with her 3 indoor cats.

Participant Biographies

David Bowles
B.A., LL.B, Public Administration and Law; GDLP, Certificate in Project Management; Harvard's Office of the Vice Provost for Advances in Learning Certified in Cybersecurity: Managing Risk, ACLI Director and Board Member, ACLI Member

David Bowles is Special Counsel, Ethics at the Queensland Law Society, and since 2017 has been the Society's lead cybersecurity author.

Admitted in 1996, David has extensive general practise experience, focusing on technology, property and litigation.

David is a regular contributor to Proctor and has a keen interest in cyber law and security in the legal sector.

Michael Hill
ACLI Member, Director and Board Member, Founder of Regulae Systems

Emma Watson
LL.B., B.Com., GDLP, ACLI Member, EWOWC Member,
Co-Chair – Cyber Security Submission Working Group

Emma Watson is a Law Graduate at HHG Legal Group who specialises in Commercial law. Emma is passionate about the role of information technology in legal practice.

Emma graduated from the University of Notre Dame and has completed a Bachelor of Laws and Bachelor of Commerce. She was admitted to the Supreme Court of Western Australia in 2019.

Emma's current role at HHG Legal involves assisting with drafting and research about property & leasing; planning & developments; commercial contracts; and wills, estates & succession planning.

Prior to HHG Legal, Emma worked as a Legal Analyst in the Commercial & Disputes team at Herbert Smith Freehills, and has gained other legal experience within private practice at local and international firms.

Emma enjoys life with her partner in the South Western region of Western Australia including travelling for work as required.

Participant Biographies

Nick Dyson
ACLI Member, Secretary – Cyber Security Submission Working Group,
Student at Laws and Commerce

Nick Dyson is a 5th year law student at La Trobe University. Nick's focus is on the interactions of information security and legal practice.

When not involved in law, Nick is a full time discus thrower working towards representing Australia at international competitions.

Living in Melbourne allows Nick to enjoy a regular health and fitness routine, and pursue coding at enthusiast level.

Nick enjoys being a member of the Australia/United Kingdom Young Leaders Network, the La Trobe Elite Athlete program, and La Trobe University's Excellence Academy.

Cyber Security Submission 2021

ACLI thanks the Department for its request to participate in the review of Australia's cyber security regulation and for your interest in the work we do.

We look forward to furthering the discussion and strengthening Australia's cyber security position.

Contact us at info@acli.org.au and chair@acli.org.au.