Laminar

2023-2030 Australian Cyber Security Strategy Discussion Paper Submission

April 2023

Laminar

Perspective and Context

Laminar is a Brisbane based company that has clients throughout Australia. Our submission is based on our engineering experience in designing, implementing and operating cyber security and networking infrastructure.

We;

- Assist clients including government (Federal/State) and private organisations with their endeavours in the digital world.
- We have invested in AI based specialist tools to help keep things safe such as a sovereign Australian SIEM for mid-sized organisations. This fully sovereign service is called LaminarSIEM and provides a real time cyber risk assessment.
- We have also released to the public a free sovereign Australian secure messaging system called LamChat which is similar to Signal, WhatsApp, WeChat and Telegram.

We see daily, the impact to organisations when cyber security is not treated seriously or when the victim is preyed upon by a skilled actor. Some drivers for this could be that;

- There is a lack of sovereign solutions generally (especially in social media) which means most providers are from overseas. Who is in control? The Australian government or an Overseas government?
- The fast pace of technological development. Faster than lawmakers can deal with and damage can be done before regulatory capacities can react.
- The ability of most humans to comprehend what they are using (Artificial Intelligence for example) or doing with digital technology, is low.
- The humans in general have a desire to rush to trust.

Introduction

Technology is developing at a significant rate and those in command of it can take advantage of those who are not wise to what's going on around them.

Imagine a situation where a Prime Minister introduces a new communications "APP" to Cabinet members, that provides a secure end to end messaging system. There are troubling political times for this Prime minister also. At the same time an overseas company or organisation develops a "hack" that allows them to gain control of a user phone that has this messaging APP, by simply sending it a message request. Once in control of the phone the attacker can read messages in the APP but control other details in the phone. It can also allow the remote controller to enter messages and send them to other members of the chat groups as if from the hacked user. Imagine a party room uprising that is organised over that messaging system (APP) and the Prime Minister is outed. Who could organise such a thing?

Imagine an AI based application operating from a human's internet access device (a phone) that is able to mimic human behaviour and to be the human's friend. Imagine the AI system operating in the phone has a higher knowledge capacity than a human and is running algorithms to manage or manipulate the psychology of the human. To whose benefit? What if this AI friend convinces the human to do or not do things based on someone else's agenda. How would the human know? Will the human defend the friend?

There is so much potential (both good and bad) with the adoption of modern technology. The impact to human kind will ultimately be determined by how humans use it. The Australian Cyber Security Strategy could have a big impact on the lives of Australians in the very near future.

We are very optimistic for what digital technologies can do for our future, and we embrace the efforts of this strategy submission to balance the advantages of the digital economy with the potential risks of misuse and protecting people.

Who Controls the Humans?

Technology is moving quickly at the moment with the release of ChatGPT and OpenAI in November 2022 as an example. Making laws about any specific technology could be futile. In many cases, by the time laws are enacted, the technology could have significantly changed or been outdated. Therefore laws might need to be more subjective and be considered, for example along the lines of regulation of company director obligations, such as maintaining a safety culture. That is, if a cyber or services provider does the wrong thing by society, it will be banned or punished in some way.

The impact on society could be significant. Whoever controls the Oblong controls the humans! This is partially a reference to the futuristic world in Clara and The Sun, by Kazao Ishiguro. The advent of the mobile phone, tablet or computer as the main source of input and communications for a human being means that decisions made by the human are significantly impacted or controlled by this technology.

Modern AI is so good it can outpace humans in many endeavours and has the ability to create false perspectives at high speed. Most humans generally struggle to determine what's real online and can be easily influenced. The impact of the likes of Cambridge Analytica are well known but the technology is now widely used by digital marketers, pollsters and political parties.

The prospect of AI friends (like Clara and The Sun) for human beings that are virtual "Oblong" based systems is very real or already exist in some forms. The control of these will be highly sought after as humans will trust their friend over other humans and other presentations of reality. It is likely that these will be or could be controlled by AI algorithms. The combination of this capability with existing technology such as processing speeds, "big data" and psychological profiling (Cambridge Analytica) will be very powerful.

How do we deal with:

- The vulnerable?
- People who are psychologically affected or groomed (potential extremists) from tainted feeds in social media?
- The elderly who are not tech savvy?
- The young? (Learning how to use technology safely)

The struggle that many in the cyber security industry face is with human behaviour, not technology. The rush to trust in human nature is our biggest behavioural issue to deal with.

Bolstering Australian Capabilities

In defending the country, the military leaders we have met say that it's important to start with a strong posture. If you make it hard to attack or inflict damage and have demonstrated capability to inflict the same in return, potential combatants think twice before starting. In modern warfare the first wave is a cyber-attack or cyber-warfare.

Certainly, the government of the day can ensure its agencies are practicing the best of breed cyber security but what about the rest of society. In cyber warfare the potential threats vary widely from psychological rallying or confusion of the human population to directly impacting infrastructure operations.

Currently, Australian consumers can become quickly engaged with the latest trendy APP that operates outside Australia's regulatory regime. The same goes for Software As a Service (SAAS) platforms and other software-based services. How do you protect Australians when you have no power to do so? By the time the trendy new APP becomes very popular it's difficult for regulators or lawmakers to shut it down or control it. Like TikTok, it's on many politicians' phones.

Once the new trendy APP business becomes large enough to create a business in country regulators can leverage the financial revenue flowing as a way of enforcing some control. We note that China bans the likes of Google, Twitter and other APPs but not the same in reverse – could Australia do the same without limiting our freedoms? It's potentially an old argument around protectionism and creating an unsustainable artificial industry domestically, but maybe things have to change on that front.

For cyber security incident response, a separate system is typically utilised for communicating in case the primary one is being monitored or somehow infiltrated. For example, if an organisation is using the Microsoft Office365 system and suffers a cyber-attack, using Teams or email for communicating would be a bad idea. In conducting our business, we suggest that Australians make use of alternate sovereign platforms for communications that are trusted in our domestic market. The LamChat system is an example.

If Australia had to stand on its own, what systems would be available for the community to use? Perhaps regulating that providers of such services (critical APPs) need to demonstrate that the services can operate in isolation to the rest of the world and do so whenever the government chooses to do so (or is forced upon it). That is, forcing a domestic capability with popular APPs and ensuring client data is domiciled in Australia also.

Bolstering Australian Capabilities *continued*

To support Australia's cyber security workforce and skills pipeline we need to find or develop more skilled people. The scale of this effort will depend on the pace and scope of our national agenda. The skill development will need to include business owners, directors, managers, ordinary civilians and the information technology industry.

The other facet to improve our capabilities is to invest in and build more sophisticated tools. This is certainly Laminar's plan in the near term by creating AI-based sovereign tools that are faster than humans and easier to scale. This includes real-time risk analysis (awareness) and automated response (reaction).

A strategy to spread the workload could alleviate pressure with standardisation and simplification to engage more people in the effort broadly. We currently observe that the ASD/ACSC Essential 8 is being used as a simple-to-use framework for many organisations to aim for and we would encourage further promotion within the community. This concept is working! It takes most organisations a year or more to fully implement a mature Essential 8 compliance as its costly and human behavior needs to change.

In parallel we certainly need to develop our national skills in cyber security and retain them. Higher wages and interesting work are always a great way to do that with technical people. The challenges are that the technology in cyber security/warfare is developing at a high pace so demand for skilled people is high and most of the mainstream technology is not developed in Australia. The additional challenge is that we operate in a highly competitive global talent market as every country is trying to do the same as Australia.

To help build a long term skills pipeline the Australian community needs to foster and support an industry of technology development. Unfortunately, this has not been too successful for Australia in the past, especially within the IT industry in general. Countries like Israel have done this successfully and now have a mature cyber industry. This may require a protectionist approach initially which may put us at odds with our allies. It's probably too late for example for the Government to mandate that all firewalls installed must be designed and built in Australia! What the government might have more success with is mandating that social media, communications and office automation solutions (sold in Australia) be domiciled, owned and controlled in Australia.

Bolstering Australian Capabilities *continued*

When we place an advertisement for a network engineer/cyber security engineer or engage in a recruitment campaign for one (which is a continual effort) we only see half the population represented. That is, the male population. We certainly have female employees but recruiting them for engineering work is difficult. We must train our engineers in any regard as very few cyber security engineers exist generally. When compared with other nations our industry colleagues overseas don't have the same problem. Some get a 50/50 split when running a recruiting campaign in Israel or parts of India and the USA. Solving this issue may take a generation but we could help our situation by solving this problem.

Boundaries and Trust

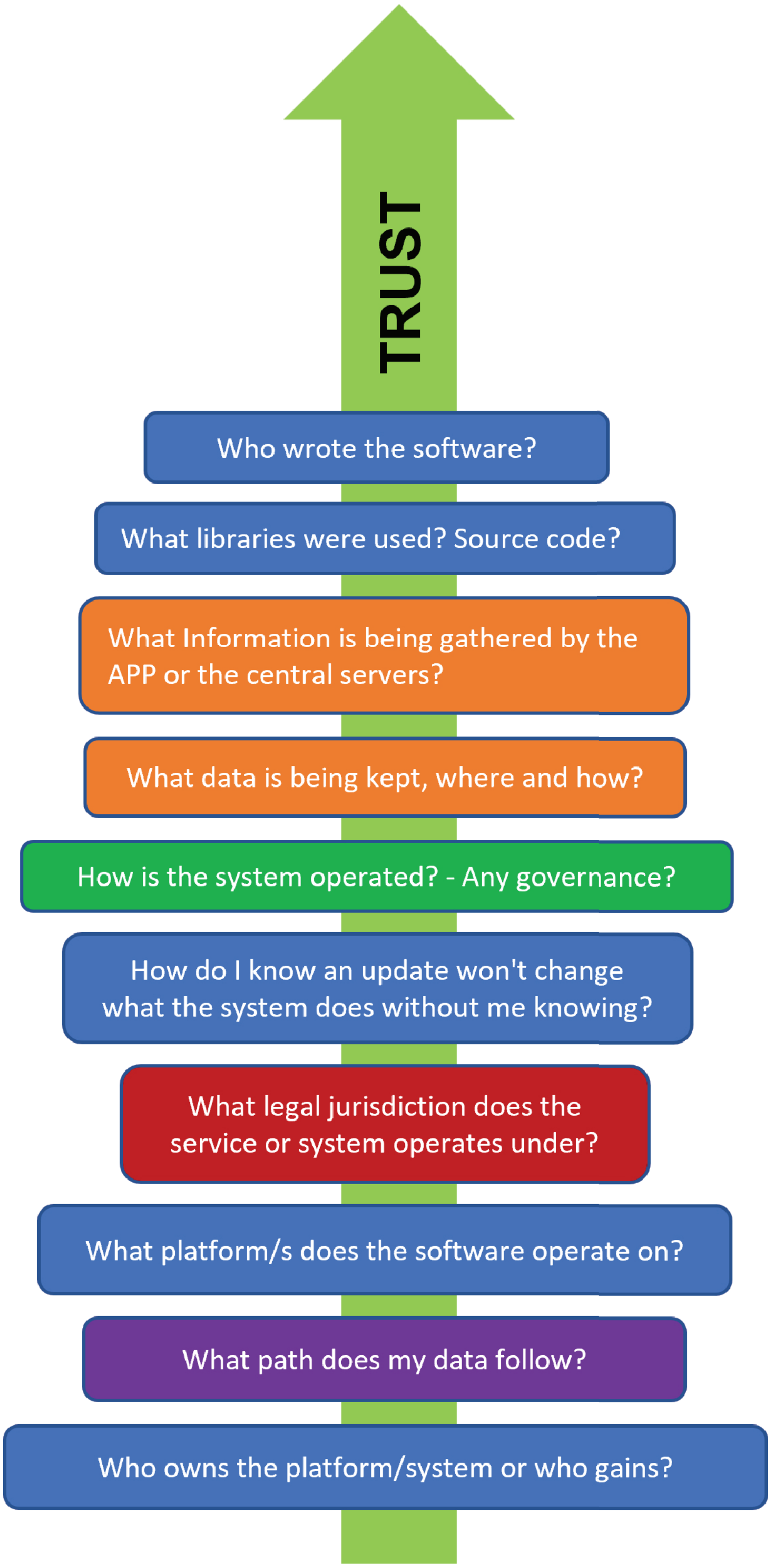
Laminar has created a sovereign social media and secure messaging platform. When creating an APP or service there are many facets to its design and operation. Typically, each of the subcomponents is open to a type of cyber-attack, intrusion or exfiltration of data. So, when using an APP, users place a lot of trust, or rush to trust to get the benefits or competitive edge of what is promised.

It is difficult for people to determine the risks they are taking to their privacy or personal information with any particular APP, even for people who are highly trained or experienced. *See the picture on page 8.* To analyse the risks, engineers work to discover and analyse each of the layers that make up the system and therefore the stack of trust. Most people don't do this when they download the latest trendy APP, nor do they have the capacity to.

To pick an example, one can visit the Internet 2.0 company site that markets a product called Malcore. It analyses APPs and presents to the user a variety of details like where the APPs connect to and how they were put together. An example on the site is the Suncorp banking APP that is created from a Huawei Software Development Kit. Many people would not know that and therefore trust it.

We would suggest that the government implement a notification or disclosure scheme that identifies the risks in each of the layers in the trust stack (depicted). Much like the nutritional details on food. A simple scoring system in each layer of the stack could provide users a basic perspective on the risks they might be taking. Initially we would expect that the government may need to test and make these ratings of popular APPs as many APPs and services are provided from overseas.

Boundaries and Trust *continued*



Who wrote the software?

What libraries were used? Source code?

What Information is being gathered by the APP or the central servers?

What data is being kept, where and how?

How is the system operated? - Any governance?

How do I know an update won't change what the system does without me knowing?

What legal jurisdiction does the service or system operates under?

What platform/s does the software operate on?

What path does my data follow?

Who owns the platform/system or who gains?

Boundaries and Trust *continued*

So many APPs that people load onto their phones offer a highly attractive outcome on all sorts of fronts like psychological fulfillment (getting likes) or access to special information when in the background the APP is doing something else like harvesting use contact lists and other private information. This information is commonly called metadata and it is very valuable.

When an organisation wants to understand what people are doing for advertising, promotion or manipulation in a digital world, they need two things. The first is to understand what is going on now, a baseline or a starting position (IE current set of information that describes the static state). Every time there is a data leak of private information this helps build a base line which is useful in its own right especially if people are slow to react or don't know data has been stolen. So much information has been leaked or stolen there is not much a government can do about it after the fact.

The second is access to data that highlights changes to the static state. Like acceleration is to velocity and velocity is to position (static start state). It's this data the government could control or regulate as it is more a flow of small information packages. Especially lots of correlative dynamic information packages. Static information ages without dynamic updates. This can be controlled by giving consumers the right to cease all metadata sharing and ensuring that any contributed content is owned by the contributor not the platform.

A quick look on LinkedIn will now show you that everyone in the IT industry is now a cyber security expert! Who do people trust?

To pick a strategy for 2030 we would need to be confident in the technology that will be available at that time. We are not sure that's so easy to pick as very few predicted the impact of Chat GPT 6 months ago. So maybe the focus should be on something other than technology. For example, develop institutions of trust that people can turn to for advice or consultation. We do this already with accountants and lawyers for example.

This means government legislative support for regulation of cyber security industry with qualifications, certifications, continual improvement and a peak industry body to manage these affairs. This could potentially start a global agenda and an education market here in Australia.

When an APP generates a certain level of local revenue, we suggest the business should adhere to Australian law and request that the system operates the system from Australian data centres.

Summary

The potential scenarios in the introduction (above) are the highlight risks the Government needs to consider controlling now. While many of these new technologies like AI offer some incredible opportunities for Australians, if misused they could create significant damage to our society. History has shown that regulation steps in typically when there is a threat to society or when people take advantage of the disadvantaged (Financial services regulation for example).

Our submission to the Australian Cyber Security Strategy hopes to encourage the Government to consider:

- Should the Minister for Home Affairs be given the power to arrest/seize/stop any service or APP that is not in the public interest. Even if it is temporary.
- When an APP or IT service generates a certain level of local revenue the business should adhere to Australian law.
- When an APP or IT service generates a certain level of popularity (number of users), require that the system operates the from Australian data centres.
- Create a rating system around the “Stack of Trust” for APPs and IT services like film ratings or food nutrition notification.
- Find a way to encourage women into our work force especially at an engineering level.
- Support domestic created solutions over foreign and maybe the government only use sovereign designed built and operated services.
- Create or support a peak industry body with legislative backing with certifications and training to create a trusted industry like Accountants or Lawyers.

Laminar

About Laminar Communications

Laminar is a Brisbane based company that has been operating for 15 years. We are a highly technical group of people and we relish in helping our clients make sense of the complexities of modern IT networking, focusing on cyber security, networking and wireless communications. Laminar currently provides a sovereign MSP SIEM for mid-tier organisations including Federal government departments as well as engineering resources to help organisations build cyber security infrastructure.

Laminar also has released a free secure messaging service to the public called LamChat. It competes with the likes of Signal, Telegram and WhatsApp, except it's an Australian sovereign solution and more secure. This culminated in three years of work and a way for us to give back to our society. Now it's used by people in defence, ASD, cyber security organisations regular companies or organisations and the general public. LamChat is more than simple text messaging. It is also used for file transfers, video conferences, broadcast channels, sharing photos and videos as well as other social media applications.

Laminar Communications Pty Ltd
+61 7 3177 0899
www.laminar.co