DEVELOPING A COOPERATIVE APPROACH

To Digital Transformation and Security

Between Governments, Public Sector Agencies, Institutions, Business

And individuals in the wider community

Awareness, Vigilance of and Countering

Identity theft, fraudulent identity breeder documents, money laundering, criminal activity and terrorism funding, Internet predation and dangers

Kevin Beck

Melbourne Australia

Mobile: [redacted]

Email: [redacted]

EXECUTIVE SUMMARY

I have concerns that the existing frameworks of the Australian Government and agencies such as Attorney Generals, Prime Minister and Cabinet with the Digital Transformation Agency and the Cyber Security Centre, Defence DSO among others are inadequate.

This is particularly heightened by yet another recent multi-million-dollar key ICT failure – biometric identity in the Crime Commission and DTOs public service wide identity proposal.

I AM PROPOSING that the Digital Transformation Agenda of the Australian Government incorporate a wider involvement by all sectors of Australian society and economy.

Any framework will be impacted, and made more challenging, by the implementation of the National Broadband Network bringing with it a new set of challenges.

Australia's public-sector agencies handle, process, issue and store vast amounts of information and this should be coordinated and centred in a secure facility and operated much like a private bureau that produces driver licences, financial cards and other critical instruments.

Criminals, of all persuasion, are effectively using the fractured structures and the disparity in security that exists across the nation.

The private sector has built data centres to variable standards. Some have Australian Defence Department classification with most adhering to NIST standards. They all focus on cloud services for the security with the fiscal attraction being a lower cost to the public and corporate purse.

This paper poses, and looks at Australia's security, in a broader world context framing the issue of data security and document issuance within the sophisticated activities of criminal networks operating across borders and sovereign states, operating within legitimately and illegitimate cohorts and communities blending in so to speak down to the individual level.

I believe a sophisticated global criminal structure has been built in front of us and a majority of Australians do not see it or are not equipped to deal with it.

In 2015 - 2016 I Issued multiple, extensive materials to AUSTRAC, Attorney Generals Department, Prime Minister and Cabinet and Finance and submissions to Parliamentary Enquiries indicating that legislation and regulatory attention was not of a nature to inhibit, deter or stop criminal activities.

- The facilitation of money laundering by Australian Banks and financial institutions supported by credit and debit card machine manufacturers and issuance bureaus
- The facilitation of money laundering and tax evasion by retailers selling gift cards, prepaid debit cards, for any amount, with no limit, without requiring identity production by the purchaser.

THE LOCAL IMPERATIVES

The Australian government, through its own agencies, is a user and issuer of secure data, documents, services and systems, evolved out of a myriad of sources of data in-house and external. External source data may be private individual, corporate, other jurisdictions of governments and many others including international.

In terms of the Australian government itself, the question arises as to how this extraordinary amount of data can be filtered and allocated a security level according to its purpose. The debate may revolve, inter alia, around what data should be centralised, and operated, on and what can remain distributed in the field and outwards to the public.

In turn what data comes in from the public and how is it classified?

I see a much wider risk and concern, not only with how Australian states, territories and local government manage data storage, privacy and activities but how commercial enterprise, and Institutions as well as individuals, manage their own and how the whole is being manipulated by criminal elements.

A disparate patch work quilt of policies, and actions, by government and key sectors of business enterprise (banking, utilities, telecommunications, document issuance and so on) serves to advantage criminal elements here and internationally.

Australia's Local Government, Other Agencies and CERT Australia

I acknowledge the roles of Prime Minister and Cabinet Cyber Security Policy Group, ACSC and others in the structure of the Security Policy and Coordination (CSPC) Committee, which is the interdepartmental committee that coordinates the development of cyber security policy for the Australian Government.

From out here the creation of the Digital Transformation Agency has blurred the boundaries and made responsibility unclear because DTA is a technology focused agency and not a security agency in my view.

One might assume, or external parties in the private arenas described above, may claim, they have a similar philosophy as the government in defining measures relating to the confidentially, availability and integrity of information that is processed stored and communicated by electronic or similar means. They may claim to share the aim of the Australian Government's cyber security policy in the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy and that Digital Economy is to be enhanced by the National Broadband Network Capabilities which will bring greater challenges to the Government's Digital Strategy.

Much of this cooperation, and shared, views are rhetoric and subjected to the limitations of cost and priorities. Down at the Individual level it is more of being oblivious.

Australia's national security, economic prosperity and social wellbeing are critically dependent upon the availability, integrity and confidentiality of a range of information and communications technologies (ICT). This includes desktop computers, the internet, mobile communications devices and other computer systems and networks and may I add products that are provided by external parties such as passports, employee identity, smart cards, tokens, credit cards and any other instrument that deals with data including wearables.

We can all cite an increase in malicious code, attacks and criminal activity, as is particularly the case for financial transactions and sensitive commercial or personal identity including theft thereof, or the creation of one core document to breed others for the purpose of opening a bank account, a social security identity, a driver licence and more.

- The 100 point check where the Medicare card, and a utility bill, is a significant score points to a ludicrous assessment of identity
- Australia Post's adventure in identity along with a myriad of other offerings adds to the disparity. Though pundits and promoters of competition would have us believe that the risks are diminished if we have a common standard.

Many involved in data, privacy and protection, noted during the Access Card exercise the resistance to, and misrepresentation of, efforts involved in confronting and managing risks trying to balance them against the civil liberties of Australians, including the right to privacy, and the inherent need to promote efficiency and innovation to ensure that Australia realises its full potential.

This task is compounded by vested interests, and users, who are free with their private information on social media, perhaps not fully understanding the dangers though with the Facebook expose and the EU's GDPR a major awareness is appearing.

The corporate response has been to confuse and seek to maintain controls through superfluous privacy documentation measured by volume.

Australians are also somewhat cavalier with the cards, passports and other identity instruments that they treat as every - day items but which are more and more the targets of criminals.

- Whilst decrying an Australia card they are happy to hand over their privacy to Apple, Facebook, Google and any other tech offering a free service

I am moving beyond the mere concept of a Cyber Security Centre supporting the government's objective of cyber safety focused on protecting individuals, particularly children, from offensive content, bullying, stalking or grooming online for the purposes of sexual exploitation to a broader economic and social context, requiring coordination of other related policies, programmes and industry participation. There is a role for industry, community and individuals, in this scope in the federation of competing interests, and knowledge awareness of federal, state and territories.

WHAT AM I LEADING TO?

A global network of criminal elements has emerged, literally coming together like a new generation mafia, using whole countries (pariah states, states under sanctions and so on) whilst integrating their activities into institutional structures (politics, government, banking, financial systems, utilities, technology and telecommunications, social media and IoT) across the world, including Australia, to launder large volumes of money, to create fraud and as we know to fund terrorism and to create nation state advantage.

They masquerade as legitimate.

This is not simply the transactional movement of funds involving the complicity of a bank, or other structure, it is the actual manufacture of the foundation (the Internet hardware and software) for that movement beyond data transfer in computer systems and on the Internet out to physical instruments such as credit cards, chips in mobile devices and wearables.

- The use of technology in banking, particularly fully autonomous ATMs that can accept cash of up to $5,000 in notes and the CBA machines that handle $20,000 and disperse it across the world in milliseconds has been obvious for years yet who took any action to stop it?

The clients of these outputs, and their supporters, are those who embrace serious badness.

Every honest business, and person with integrity at their core, would support the National Leadership approach by the Australian government within the federation of a shared responsibility in the communication, and storage, of sensitive information (of all types) and the obligations of mutual respect for the information and systems of all users.

However, despite the rhetoric the permeation of honesty in Australia's corporations is not all that obvious. There are detractors:

- Shareholder's interests before public interest
- Bonuses that test and override moral imperatives
- Disrupters who believe it is fine to ignore laws, regulations, traditions and people's livelihoods whilst also threatening national security

Not only the public service should be engaged, through knowledge leadership and action, in a partnership approach to cyber security and public interest protections across all Australian governments, the private sector and the broader Australian community is seen as essential along with our nation's allies and multi-national global corporations that cross borders.

Globalism supports many players and is a major fillip for the criminal person and the criminal state. We have for decades installed disparate systems in government to produce identity, across a myriad of agencies in Australia, all with varying or no level of security we are now also building a mechanism (the NBN) that will be of great benefit to them.

- The transfer of responsibility for identity to the DTA is in my view not an effective policy to overcome fragmentation or to centralise because as stated previously DTA is not a security agency and it is not one that has a natural interaction with business, community and individuals.

I know they do not interact because DTA never responds to my communications or white papers whereas PM&C do on every occasion and with swift response.

Australian government, via its agencies along with Police, Regulatory Agencies, Australia's states and territories, and companies, that have global operations can support, and add value to, the Australian Government's international policies, strategies and initiatives and can garner support from business and individuals.

All business, just like Australia's Governments, requires risk management in a globalised world where interoperability and internet-connected systems are potentially vulnerable and where cyber - attacks are difficult to detect, there is no such thing as absolute cyber security.

However, on too many occasions, entities operate in a state of unawareness of what human and machine networks they are in and supporting, knowingly or unknowingly. Human error is the greatest risk

In concert with government, and community, **everyone must be brought into the policy and the intelligence exchange, to the extent they want to participate**

This would require teaching individuals how to apply a risk-based approach to assessing, prioritising and resourcing cyber security activities within the values paradigm of their individual operations, cultures and perceptions. And I do not mean TAFE courses.

Why are there not public participation centres in every state and territory?

Collaboration is a preferred style by many in corporate life, but this does not work effectively since it is largely lip service.

- A majority in the community neither have the inclination, awareness of technical knowledge to create a national fabric of security and awareness
- Citizens do not easily interact with government agencies
- Criminal activity, tax avoidance, paedophilia, content and identity theft are all rife from individuals, SMEs into larger organisations – public and private
- The dark web lurks
- People who might want to contribute are shut out by vested interests and public service culture and modus operandi

- Those who speak out or do not conform to their mores and approach to dealing with Government and the Australian Public Service largely through risk aversion and self-interests are punished

Many enterprises educate employees, and customers, as to the cyber risks of instruments that individuals carry and use. As a part of their own cyber security they must operate, and maintain, secure and resilient information and communications technologies to protect the integrity of operations and the identity and privacy of the customers and end users. This vitally includes corporations engaged in the manufacture, and distribution of critical identities.

The Australian government, and other jurisdictional agencies, NEED TO MOVE TO educating, and empowering, all Australians with the information, confidence and practical tools to protect themselves online and in their financial and other transactions against the hidden criminal operations described previously that pray upon ignorance, greed and human nature.

Australia's Governments may promote security and resilience in infrastructure, networks, products and services across governments, including parliamentarians, associated people, employees and communities but this is but one part of the puzzle and vital mosaic that builds to protect our nation (as a whole) and our cooperation with like - minded sovereign states.

The private sector, and government agencies the world over, look to the protection of their ICT systems but to what extent do they ponder how criminal elements become embedded and institutionalised as part of those structures? Criminals take live (or deceased) identities and data to manufacture other things for their needs and then send them into the legitimate world.

Significant Australian companies and, more particularly, those with global footprints could, if they were prepared to, work with CERT Australia to assist the owners, and operators, of Australia's critical infrastructure, and systems, of national interest and add support to CERT Australia within the global community of computer emergency response teams (CERTs) to support international collaboration in regards to cyber security issues and also complement the work of the Cyber Security Operations Centre within the Australian Signals Directorate. These collaborative arrangements can also serve to make participants aware that their business can also provide the foundation and tools of crime and terrorism and to incite them to vigilance.

A sort of crime stoppers corporate world that flows down into community and the individual level. Individuals learn much about security from their employers and jobs.

The identity technology providers to which I speak above already support the work of the APS agencies in the area of identity security and production. Many companies work with CIT integrators who are also engaged with, or embedded within, key agencies.

However, I would put it to you that it is into these legitimate structures the criminals have entered masquerading as good corporate citizens. Not only criminals but also nation states. The banning of Huawei from participation in the Pacific Islands undersea cable connecting to Australia is a case in point.

The work of the Department of Broadband, Communications and the Digital Economy, and now Prime Minister and Cabinet through the DTA, and the implementation of the National Broadband Network (NBN) raises opportunities for the promise of collaborations and of particular focus for my area of interest, **how data is to be sent across the NBN according to the user profile?**

There is obviously an expectation that the private sector will embrace the NBN on the proposition that the NBN will greatly enhance the transportability of data and at the same time the activities of the criminals. We know today's sophisticated criminals do not wear black hats and long coats all standing out in the open for us to see.

We must educate individuals global network that is operating out in the open.

Although the network connection between a user's web browser and the server is purportedly secure, it is unlikely that a majority of people even SMEs use keys and encryption, and therefore the user data is kept in clear text at rest on the host servers and can potentially be viewed by anyone with the correct level of access. From this they can take data files to populate the instruments I have referred to which in turn form the mechanism for movement of funds and data.

This poses problems for governments, organisations, and individuals who wish to store and exchange sensitive information, patented materials and sensitive private data, such as patient medical records, identity instruments, passports, driver licences, and credit cards, financial security instruments printed or electronic.

Most companies, and agencies, dealing with critical business use, inter alia, plug-in technology that transparently intercepts the user data prior to it being sent to the distribution server and encrypts it. Not everyone wants to encrypt a document but there will need to be options to do so. Sharing documents, and data packages, is a significant consideration in where servers are connected to government and private sectors receiving and transmitting data.

THE INTRUSION OF CRIMINALS AT EVERY LEVEL

What is the mechanism by which Public Service Agencies, Businesses, Organisations, Institutions and Individuals become aware of the intrusion of the criminal if their requests are merged in with legitimate packages of data? Data going from banks to card issuing bureaus, data going between public service departments, data going LAN and WAN

An example of this is the exposure of local, and global banks, facilitating the laundering and transmission of large volumes of cash on behalf of drug cartels. The people in the drug business use credit cards. Suppliers of identity technology happily sell their equipment to Iran and other pariah states. T

They are simply part of what appears to be a large stream of legitimate issuance by third party providers knowingly or unknowingly. The former (knowingly) is the challenge where the illegitimate dress up as legitimate. Of course, this is not the case with technology installed in criminal nation states where the equipment and technology is dedicated to the sole purpose described.

Here we can expect that criminals are studying all they can about the Australian NBN, public service and our businesses including SMEs, structure and security.

- Cyber-attacks rain down from everywhere.
- Opportunity knocks for the invaders.

The level and type of encryption cipher may be of key consideration in the Australian NBN as it seeks to provide a transport highway for mass movement of image, voice, data and text.

But who is focusing on how security is ensured from the start point at the individual and SME levels?

Then there are considerations where business, and other users, want to access their documents from any machine (in the cloud) as long as they have the appropriate plug-in installed. In amongst all the traffic is the parasitic criminal, plying its trade locally, nationally and internationally.

No doubt the technology focused in DTA and other agencies, such as Health and Human Services, along with industry, will look to user decryption keys and user-chosen passwords or an appropriate level (1 – 4) of authentication which may or may not be mandated but these are aimed at the legitimate and will be irrelevant to the criminal who have embedded their activities into the legitimate world.

- It should not be readily accepted that people will embrace facial recognition once they understand it fully

Multitudes of document issuers are developing their own software with extensible functionality to encrypt outputs and transactions. They manufacture, personalise and encode identity instruments embedding logical and physical authentication devices, interfacing to biometrics, public keys and third party issued security certificates. These are manufactured according to the end user requirements. Government agencies, and others, utilising government servers, portals and end to end services across the NBN may be required to use FIPS, HTTP and other protocols including authentication levels of verification. These are freely available and are used for the production of identities to serve criminal ends.

Education is vital in implementing Australia's Cyber Security model in its fullest sense down to individual level.

But beyond this I believe that Governments must engage the vigilance of "good and honest" people in industry, and community, share and garner intelligence on a scale never before contemplated.