Department of Premier and Cabinet

Privacy and responsible information sharing - submission

"The pervasiveness of the internet means that once personal information is released into the public sphere, it can be very hard to control the use of that information." (hon. John Quigley MLA , Attorney General; Minister for Commerce)

"Global cyber threats have never been more aggressive." (media statement- leading USA cyber security corp, Symantec, Aust Financial Review 2019)

"there has been an unprecedented amount of cyber hacking in the last few years." (Dan Tehan, Minister for Education, ABC TV October, 2019)

The hon John Quigley has provided the truth on the most crucial issue on the storage, access and sharing of internet data information, particularly personal information. ie "Once data is released it can be very hard to control the use of that information." the Symantec quote confirms the hon Minister`s truth quote and emphasises the cyber threats are escalating. The greater the release and accessibility of personal data, the greater the risks increase for data being hacked, sold, marketed and involved in id fraud.

I assert no government, or any corporation will in a customer, public contract guarantee the 100 percent privacy security of personal data in data bases, being misused and shared with no consent with third or more organisations. Thus, I do not accept or agree with the WA govt proposals for greater collection, storage and sharing of my personal data via a new internet central data base that will no doubt require registration and an id pin access that needs to be changed regularly.

It is very clear and obvious in the proposal document the WA govt is intent on establishing a centralised personal data base state wide that is substantially in the interests of all govt departments, including linkage with federal govt departments. The basic privacy wording, is just a pr message to seduce the public some how the WA govt can achieve what no other govt, or multi national agency has been able to achieve - no government, or any corporation can, or will guarantee the 100 percent privacy security of personal data in internet data bases.

All governments and particularly corporations are collecting, storing and sharing personal data, because it is the new gold product for marketing, advertising and selling. Also, no doubt website data bases have dramatically reduced organisation operational data use costs and provided an increasing annual income stream. Thus, the WA govt will establish the centralised personal data base regardless of no public user contract 100 percent guarantee personal data will be totally secure and regardless of public submission rejections. An ABC radio guest commentator on the WA govt proposal stated all state governments at a previous COAG meeting (2017) had agreed to establish a central personal public internet data base to share data with a federal central data base concerning all departments. ie the current federal legislation proposal for a new personal id data base website developed by the home affairs dept that has been initially rejected by a parliamentary committee, because of quite inadequate privacy and data regulation provisions. The id bio tech system is reported as not fit for purpose. Personal id data sharing no doubt is expected with the DSS, my gov, ATO, home affairs and federal police. The WA govt has not disclosed to the WA public the data sharing agreement with the federal govt in the WA proposed legislation.

I have read in the financial review in the last few years the DSS and my gov website public data base websites are dysfunctional and the federal govt has expended hundreds of millions of dollars endeavouring to resolve the issues with limited positive changes. I have also met people that have engaged in the stated websites and they have confirmed the information provided in the financial review information. Regardless of the dysfunctional websites the federal govt has virtually made it compulsory (tech autocratic citizen oppression) for all citizens to engage and comply with the DSS, my gov and ATO websites.

<u>Cyber hacking breaches - major evidence examples</u>

There has been a broad range of publicly disclosed corporate and government organisations that have been hacked for personal data misuse, exploitation and fraudulent behaviour. ie the Apple cloud storage personal data has been hacked in the USA, including Google, Facebook data bases and the USA Pentagon data base system. Also in the USA small companies as in Australia have been black mailed for payment demands to release computers from ransom ware control. Further, in the USA the media has reported 500 schools` computer systems have been hacked, including 170 local government cities.

The media has reported the computer health data system in Singapore was hacked in the last year.

In July this year the federal police department was reported in the media for 100 breaches of personal data access to website meta data without obtaining the necessary court warrants. There has been no reports of any particular police being charged for an offence, sanctioned in any way, or terminated. Thus, once personal data is accessible on internet data bases the risk is high the data is liable to be hacked even by police without approval and with no apparent consequences.

A substantial computer system hacking during the year was at the ANU where it was estimated over 200000 staff, student personal data records were hacked regarding a period of 19 years. No offender organisation, or persons have been really identified, or apprehended. Recently this year the billon dollar corporate organisation CSL website data base system was reported to have been hacked. No offender organisation, or persons have been really identified, or apprehended.

The media has reported only an estimated 27 percent of Australian federal government departments have established some reasonable cyber security protection. No surprise, the media has reported cyber computer website crime costs an estimated $29 billion dollars per year in Australia.

It was reported D Watt the Privacy Commissioner in Victoria acknowledges government departments want to engage in personal data sharing, but they do not have adequate computer system cyber security protection.

There is no mention in the proposal document how the WA government is going to really make personal data more secure and privacy protected, especially in relation to the hon john Quigley`s quotation. ie personal data being hacked, misused, transferred, sold/marketed and id defrauded from the govt, corporate organisations presented in this submission.

The WA government in association with the federal government is becoming an emulation of the Chinese Communist Party collecting personal data surveillance of its citizens 24/7 via CCTV, i pad, mobile phone and pc website connected devices. The federal government is the only OECD govt that has legislated the AFP authority to access encrypted website and tech data apps ie governments are establishing a personal data tech autocracy.

Conclusion and Recommendations

It seems clear the WA govt is intent on establishing a central public personal data base online website that is accessible to all WA departments and federal govt departments. Most likely local governments will also access id data sharing. The latter is regardless of the confirmed data hacking, id fraud risks, including any substantial rejection of the proposal in the public submissions. It is quite unacceptable that the WA govt has not disclosed to the WA public the 2017 COAG agreement to share id data with the federal government. Why not?

No government, or corporation can, or will provide a 100 percent guarantee their website data base storage, access and sharing is totally cyber, privacy secured.

A real issue for WA citizens regarding confirmed id fraud is that the transport dept has no provision, or acceptance for the need to enable vehicle drivers to be given a new driving licence number to cease ongoing id fraud financial liabilities. WA govt needs to act on the latter legislation, regulations amendments asap.

The proposal for a privacy commissioner effectively confirms the WA govt expects their will be public complaints about cyber security issues eg alleged misuse of personal data, selling/marketing of personal data and possible alleged accidental transfer of personal data. I recall some years ago a previous alp government was reported in the media regarding the transport department being identified for selling at least 20000 personal data documents to the private sector. I do not recall any media report that any department staff, management or the minister experienced any sanction consequences for the unethical breach of peoples` privacy details.

The proposed data sharing legislation document does not mention any range of sanction consequences for department management, staff or any organisation that is identified for privacy misuse, selling/marketing, fraudulently misusing, or accidentally transferring personal data. Consequences need to range from financial costs, referral to police, suspension of employment for review and employment termination, including prison term options. Mandatory legislation conditions.

The best practice real privacy of personal data is that people voluntarily provide their data to a department, or any organisation and the best available ongoing security tech systems store the

data and all data access staff have clear police regular offence records. All other departments and organisations also need to have installed the best available ongoing security tech systems storage for the data and all data access staff have clear police regular offence records. Mandatory legislation conditions.

All proposed personal data sharing to any other department, or organisation regarding identified, and de identified data needs to be formally disclosed to the people concerned for their written documented approval for their data sharing to be provided. All information justifying the reasons for the need for the personal data sharing needs to be disclosed to each person concerned. Any monetary payments for the data sharing also needs to be publicly disclosed. Mandatory legislation conditions.

With respect to the public providing notification changes to a central WA govt website only once for all relevant departments, the current facility of being able to provide one email with multiple department addresses means this alleged benefit of the proposed new govt website data base is not valid.

As the financial review in the last few years has reported the DSS and my gov website public data base websites are dysfunctional and the federal govt has expended hundreds of millions of dollars endeavouring to resolve the issues with limited positive changes. Can the WA govt guarantee a WA personal data base system will be able to prevent being dysfunctional at any reasonable costs compared to the federal govt experience?

The WA government really needs to contract the best independent most relevant corporation to seriously explore the economic costs, citizen privacy data risks costs compared to the benefits of the proposed WA website personal data base department, agency sharing system. Eg AlphaBeta. A mandatory legislation pre condition report for public disclosure and for voting at the next election.

As we are living in a democracy, all public citizens need to have a choice whether to comply with the proposed new govt website data base technology the same as the choice provided with the federal personal health data base records system. People who do not voluntarily opt in to the new WA personal data base website sharing system should not experience any negative sanctions for not engaging in the new proposed govt website system. Thus, the WA government needs to ensure our democracy is not becoming more and more like the Chinese citizens` surveillance id data tech autocracy.

Albert Einstein has said, "Insanity: doing the same thing over and over again and expecting different results."

Yours respectfully

Graham McPherson

Advocate for over 36 years

Halls head WA 6210