Comments – Part one

Should I police my interactions with my doctor?
With this Open Data legislation giving the ability of Big Pharma to rummage through my doctors private files I feel violated.

I would like my medical data destroyed as it is no longer necessary. My interaction with my doctor was on the assumption that my interaction was private; this legislation significantly changes the terms and condition and retrospectively moves the goal posts that I was making my decision with my engagement and frankness with my doctor.

Medical data is particularly easy to re-identify.

A CT scan is like a fingerprint. Gene testing is even more precise than a fingerprint. What are the protections when the new field of selecting drugs by using DNA genetic testing and analysis becomes more widespread? There is also a whole new field that reconstructs a person's identity, could this be used to profile potential future criminal behavior? Can police and security services access this data?

Powerful and beyond the law, "researcher", Google and Amazon with billion of data points and a terrifyingly capable Ai when combined with heath data is an extremely uncomfortable thought. No data is anonymous. We will lose Australian sovereignty over our data. Our privacy will be betrayed. There will be a lot of lobbying and pressure from Google for access, it would be worth many billions if properly exploited over the next 100 years.

I would like you to consider the above when developing the legislation, as once data is released you cannot get it back.

Comments – Part two

Open Government & The Social Credit System - Dangers of the Backlash of a Stressed and Micromanaged Population

Inter agency data transfer opens up the possibilities of agency surveillance in the future

Australians feel that they are losing control of their world. To reclaim back some control of their lives many are tuning to alternative perspectives and theories. Government and institutions, up until recently, is were Australians looked for reassurance and safety. I have sadly noticed that many rational Australians are attempting to regain control of their world by clinging on to various conspiracy theories. In the community many have little trust in big data sharing

Open Government sounds like clever double speak for an Orwellian system to micro-manage the people. Australians and media are shocked and in disbelief at the use of the Social Credit System overseas the feeling in Australia is that it is so outrageous that it could never happen here. However in reality Open Government is just one application or mouse click or bout of creeping agency authority away.

The legislation must be unambiguous in that it that makes it impossible for Big Data citizen control and manipulation to happen. Once implemented it will be here forever. A future tyrannical government could use it against opposition or troublesome politicians or citizens. It would be a

failure of imagination to not envisage all the unknown unknowns.

There is a danger this system creates a disenfranchised population stressed under unfair control and relentless application of the rules and laws from the system. Robo-debt was a tiny example of what could go wrong which was a mild example of the failure of building trust in data sharing.

In a Catch22 the system may then become necessary to use Open Government to discipline the now disenfranchised population. I feel this project is ignoring this rudimentary Achilles' heel. It would be better if this major issue is honestly head-on addressed in these initial stages rather than becoming a perpetual Sword of Damocles perpetually hanging over the Government and various agency heads. A centralised data system could turn into an ongoing political and social disaster.

****

In the AG's Office presentation it was clarified fraud is being defined here as fraud by the individual against the Commonwealth, not by corporations against the individual or Commonwealth or States. The AG Fraud prevention centre started 2019 is to build capacity against fraud and it provides tools to agencies to connect them to enforcers. Andrew Walter the First Assistant Secretary gave an indication that some of the tools that would or could in the future be used for darbyshiring and scraping data from all Open Data agencys and the private sector such as banks. The term tools are very broad and rings alarm bells. In Xinjiang the Integrated Joint Operation Platform" (IJOP), uses pattern matching and artificial intelligence tools looking for "micro-clues" to identify incohesive behaviour and "illegal activities" it is a powerful interagency tool. Australians and our media are in disbelief at this system.

Open government is just one application away from an IJOP. Many of us studied Orwell's 1984 at school, it was for a good reason; it was to insure that as adults we are alert to the dangers of highly a centralised, dehumanised societal enforcement system. We must be very wary that what of opening this Pandora's Box of automated data driven justice.
Robodebt was an example of clumsy pattern matching, data errors, have destroyed peoples lives. Some of the outcomes have been fatal.

Once it is opened it cannot ever be closed. Without clear open and publicly debated ethics policy and board of what is acceptable there is a real possibility that before we blink we ratchet ourselves in to our very own Australian IJOP.

Comments – Part three

Data mishaps are a major threat to building trust in data sharing.
My experience with data handlers is how unaware many are to the risks of handling data, this appears true in civilian street as well as in government and business.
At the very least I propose a Data Handlers License which should be required for any one handling over 1,000 personal records (with online testing like a NSW RSA) and big business or government data handlers should be required to have a higher-order qualification (such as accountants are required to have to handle money).

Some of the issues that are essential:
*Responsibilities required under the law for data handling and the maintaining of values to uphold civilian expectations.

*The awareness of how third-parties such as researchers and contractors could mishandle this data.
*Understanding that all anonymised data can be re-identified.
*The consequences of poor judgments, to the individual, national security and trust.
*The requirement to only hold only just enough data for agencies to carry out their work, a large data foot print exposes us all to more manipulation when a data breach occurs. It should be assumed that at some point in time a data breach WILL occur. A cost / benefit should be made for every line of data held.
*Exposure to legal liability
*How social engineering can trick data handlers to release data or security keys. Internal staff risks.
*An understanding that data security software becomes increasingly obsolete from the moment it is implemented.
*The clear understanding of the threat to national sovereignty and the vulnerability of having a high value a honey pot of centralised data and the dangerous opportunities this gives third countries and bad actors to weaponise this data against us.

Without professional Data Handlers our faith and trust will be shaken every time a handler make an uninformed but honest mistake.

****
At an Open Govt workshop it was suggested by Peter that the anonymised data could be used by researchers. To be honest I was shocked that someone handling data in 2020 would not be aware that re-identification is a certain reality.
Here is a research paper from back in 2012 which shows as far back as 1997 low-tech re-identification has been possible. https://fpf.org/wp-content/uploads/The-Re-identification-of-Governor-Welds-Medical-Information-Daniel-Barth-Jones.pdf

Google is a researcher; controversially they have been given some “anonymised” UK NHS data to research. Google has billions of points of data some collected fraudulently or with trixy manipulation of users with its Ai and massive computing power any anonymous data could be easily re-identified. Cambridge Analytica was developed by a professor who brought his research from the noble Cambridge University in to the private political market place. I had begun a Masters Data science at UTS and interact with researchers conferences at Sydney Uni and UNSW not all research is benign.

No data handler should be let anywhere near data if in 2020 they still believe data can be anonymised or that being a researcher is benign. The so-called anonymous data must remain under Australian sovereign and legal control and must be destroyed when the project is over or it could be monetised perpetually.

Comments – Part four

There must be and Ethics Board to develop policy and to debate contentious issues.

A Open log must be kept and displayed with a continuous record of all inter agency data transfers. Such as are there open continuously data channels that citizens would expect? Are there data types such as medical records that are occasionally transferd and how many time and to which agency? Australians would than have a better understanding and trust of their Government

Comments – Part five

A Lesson on Data Promiscuity

We should learn lessons from Big Data Companies.

Google feverishly collects and harvests all data but never-ever releases one bit of its valuable data. One can only buy the processed knowledge and information. Sellers are served customers without direct connection to the customers information. Google never-ever gives the actual data out. They own every one who use this data.

Facebook on the other hand was promiscuous with raw user data every man woman and their dog could use and abuse it. The result it was Cambridge Analitica who owned democracy.

We should learn the lesson from Google. Giving away data is not good it weakens us strategically.

I feel this legislation and the presentations are painfully naive and not forward looking at the long term risks that it places Australia under. Re-identified data can put refugees and their families in their home countries at risk. See the my experience in the appendix in https://releasethefuture.com/

With our regional issues it might be helpful if the security agency gave this legislation a reality check.

Comments – Part six

National Data Commissioner – Role

Our data future will have huge implications on the Australian public. Decisions made today could haunt us as a Country for decades into the future. As once data is released it cannot be clawed back.

Our National Data Commissioner has a pivotal role in ensuring the safety of all of our data. My interactions during this initial stage have not inspired confidence or that there is a clear understanding of the meta issues involved combined with the powerful conflicting interests that exist. The legislation in its broad draft stage does not address the many complex nuances that exist in handling data.

In the initial stages the National Data Commissioner needs steely determination to keep the wheels on the track. A wily hard hitter with healthy cynicism is needed to launch, oversee and advise on amendments to the new legislation. Someone of the caliber of Allen Fells would be helpful in this roll, it is defiantly not suitable for just an administrator.