December 9th, 2016.

Dear Commissioners,

At this point in the Data Availability and Use Inquiry, there were four areas regarding the Comprehensive Right for which additional information was requested in the Interim Report. We wanted to provide a follow up submission to do two things – firstly, to provide specific information to assist the Commission in those four areas and secondly to reflect on the overall goal of assisting Australia economically through better data availability and use and suggest some perspectives on governance which might assist.

Starting with the second objective. To achieve the overall goal of enhanced productivity through data we believe that the recommendations of the Interim Report will move us a long way in the right direction, but we would suggest that filling in the gaps around effective governance is crucial as the Inquiry moves towards a final report. We note the goal expressed in the Interim Report of moving from a ***"system based on risk aversion and avoidance, to one based on transparency and confidence in data processes[1]".*** We believe that in order to deliver this objective, a more elevated view of governance will be needed. We believe that data use is core to the transition of Australia to a strategic player in the information age. And the best way to dimension the governance needed is to reflect on the changes societies needed to make to manage the challenges of industrialisation.

This follow up submission was prepared in consultation with a group of global thought leaders who we asked for input and contribution. The intention of reaching out to this group was to provide the best possible input to the Inquiry. The views in this document benefit from their wealth of experience but we take full responsibility for the viewpoints expressed.

With much gratitude, we would like the following interviewees who assisted us in this response:

- Katryna Dow – Founder and CEO of Meeco.me and global speaker on data sovereignty.
- LaVonne Reimer – Founder and CEO of Lumeno.us and board member of the Personal Data Ecosystem Consortium.
- Doc Searls - A fellow at the Center for Information Technology and Society at UC Santa Barbara. Director of ProjectVRM at Harvard's Berkman Center for Internet and Society (where he served as a fellow from 2006 to 2010). Senior Editor of Linux Journal. Author of The Intention Economy: When Customers Take Charge (2012), Co-author of The Cluetrain Manifesto (2001).
- Phillip Windley – CIO of Brigham Young University, Director of PICO Labs – a group providing technology solutions that support a people-centric Internet of Thing, author of The Live Web (2011) and Digital Identity (2005).
- Lionel Wolberger, CTO of Emmett Global with over twenty years' experience of deploying enterprise-grade systems and security.

[1] Productivity Commission, Data Availability and Use, Draft Report, p.2.

Part 1 – Three Observations About Data Use

Observation #1 Data Use Is Transforming Our Society as Fundamentally as Cars

The above assertion is relatively obvious. The less obvious implication is that if we want maximum productivity for the long run then we need to invest as much in how to *manage and control* the technology as we do in *developing* it. This Inquiry comes at a time when data usage is growing every day, albeit at a far slower pace than it could and far more clumsily than it could.

There are some great references on the point that wherever technology leads, etiquette and best practice must follow. In transition periods, there is "collateral damage" which society finds unacceptable and starts to put controls in place.

We are at such a point in history. There are two binary outcomes, neither of which we want. The purpose of this Inquiry is to find a middle ground between the stark contrasts of totally free data availability and use with no controls, versus no use – a 100% private no sharing setting.

Rather than extremes, in the words of Doc Searls:

> "Instead we need ways for each of us to selectively disclosure data to others we have reason to trust, just as we are able to do the same in the physical world. So far, we lack those means. But we'll get them. Government bodies and companies should be ready and able to respond to privacy signals and agreements coming from individuals—and to respond by being trusted to obey those agreements[2]."

The driver of these efforts, now, is to enable Australia and Australians to benefit from the value of data while protecting us from the unintended downsides of that use. And as the Interim Report suggests, the key is the agency of the individual.

The evolution of the car from a faster horse to horseless carriage to today's safe and, possibly in the future, driverless cars has been the cause of major transformations in our societies. From the introduction of road rules, safety belts, blood alcohol rules, safety standards for cars, we have evolved to become more productive in our use of the underlying technology. The point being, cars enabled humans to go faster, but, in order to safely enjoy the benefits of the new technology, there were impacts and, over time, society evolved to manage those impacts.

The question, then, becomes how can we learn from our recent past and start to put those rules and etiquettes in to play faster with data than we could for cars.

Observation #2 Sustainable Data Use Is at Stake Here – Poor Governance Holds Society Back

The issue of adblocking and the approaches to addressing that are worth considering here specifically.

PageFair as of May 2016[3], reported that over 16% of the world's smartphone users (309 million) are blocking ads on the mobile web. They also report that over 298 million users are actively using adblocking browsers on the web.

Contrary to the view that privacy is dead, the phenomenon of adblocking is a spontaneous movement where millions of individuals around the world are asserting control of their data and preventing advertisers from using it. What are they reacting to?

[2] Interview 7th December for this paper
[3] https://pagefair.com/blog/2016/mobile-ad-blocking-report/

Who hasn't had that experience of making a purchase online and being "pursued" by similar ads thereafter. This is often poor advertising at its best, and arguably surveillance by its nature. Somehow, the pact between advertisers and the public has been broken. And individuals are responding.

The pity of the situation is from an economic standpoint, one might argue that advertising costs are relatively unproductive to the overall output of economies. Targeted advertising should lower search costs and make the marketplace more efficient – which arguably would be good for consumers and manufacturers. But somehow in the process of harnessing data, advertisers have managed to violate a social pact with the effect of "poisoning the well" for future marketers. This is exactly the outcome we do not want to see, and reinforces the need for a sustainable approach to data use. This is why we felt compelled to make this follow up submission to the Commission – sustainable data use isn't just an abstract concept. We are seeing the aftershocks of unsustainable data use already.

Doc Searls in his Harvard blog[4] writes extensively on this phenomenon. In an article in The Guardian, industry spokespeople suggest it is more of a customer experience issue[5], including the Head of the European Internet Advertising Board - Constantine Kamaras – who made this point about resolving the impasse in the article (although we note his bias to advertising as a social good).

"What I see as the best path," he said, "is a digital entente between users and companies that is based on quality standards and codes of conduct, but also on an understanding that all these services can only be financed, today at least, by advertising."

Adblocking is most likely only a very early stage in an ongoing evolution to enable individuals to control their online experiences. Imagine a world where browsers enable individuals to directly instruct advertisers on the level of engagement they want. Imagine a "no stalking" instruction.

This is just one example. Others include the détente required for societies to address and impose community standards on search algorithms and the businesses built around them. Recently the opaque, unpoliced biases[6] came under scrutiny in regards to search results that seem misleading and contrary to the social norms and laws designed to prevent racial and religious tension. We live in a volatile world, the last thing we need is opaque algorithms fueling tensions.

Likewise, democracies are built on an understood and constantly under threat playbook when it comes to fair elections. Current controversy surrounding the mining of people's facebook[7] data to profile them and serve up campaign messages tailored to them is all well and good. Prior to that, there was controversy of "share with my friends" type tools that aimed to recruit voters from an existing recruit's mobile phone contact books. Arguably there is a data race going on in elections around the world. That may be the case, but the civil society questions to be asked revolve around a bigger question than technology – namely - what overarching policies/approaches does each democracy want to uphold in the conduct of future elections to ensure the process and the outcomes are unquestioned.

Observation # 3 – Personal Data Is ……Personal

We will pause here to generalise the prior observation because it is crucial to anchor the discussion about governance in the context of what is at stake. Clearly adblocking was not a spontaneous reaction due to

[4] http://blogs.harvard.edu/doc/the-adblock-war/
[5] https://www.theguardian.com/technology/2015/oct/03/ad-blockers-advertising-mobile-apple
[6] https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook?CMP=share_btn_fb
[7] http://edition.cnn.com/2016/11/22/politics/jared-kushner-donald-trump-campaign/index.html
https://translate.google.com/translate?sl=de&tl=en&js=y&prev=_t&hl=en&ie=UTF-8&u=https%3A%2F%2Fwww.dasmagazin.ch%2F2016%2F12%2F03%2Fich-habe-nur-gezeigt-dass-es-die-bombe-gibt%2F&edit-text=

abstractions, regulations or the like – this was about a clear violation of a social pact. Millions of people using adblocking tools is about a visceral response – something feeling "creepy".

The truth is when we are talking about personal data, it's all about people. We, as creatures, exhibit an understandably emotive need to control how we are seen in the world and how our person is treated. Privacy, arguably, is a construct for a social animal to enable the management of different roles in the world. We have (and are expected) to wear clothes in public. Different people get to see us in different states of undress. When we have had enough interacting we can retreat inside our home. We honour in law and social convention the idea of our home as our "castle"[8]. Likewise, we have a particular view of things directly related to our concept of ourselves. Lockets of hair, through history, have had deep symbolic meaning although they are no longer in any way connected to the hair donor, it is a persistent reminder of their being. The idea of a locket of someone's hair, or fingernails, being swept up and sold for profit seems weird and creepy to most. It breaks a social taboo related to the sovereignty of the person[9].

Where does data that describes our interactions fit with our social norms? As humans, we are just beginning to examine this and need to keep reminding ourselves that, aside from the fact that technology creates the question, this is a social not a technology issue. Poor outcomes inevitably follow if social/human matters are left to specialists – this is about defining the way we want to exist together in the world. No less.

We would argue that the fact that people get so disturbed about their data is that it affects both these concepts. Uncontrolled sharing of information is like walking naked out of your front door – everyone gets to see you as you see yourself without the ability to shield and layer for different roles and contexts. And, in addition, there is possibly a deeper level of feeling that in some way our data fragments (data dust) mirror ourselves at a deeper level. We will leave these reflections for now but over time we expect the philosophers and ethnographers will dive into this (they already are) and emerge with further reflections. Putting our pragmatic economics hat back on however, these points DO matter privacy is not a throwaway term. These abilities to shield and layer identity and concepts related to personhood **are the core of our being as social animals.**

As such, the argument that privacy is dead and that the risks are far lower than the benefit of using data are insufficient. Therefore, governance of data use is crucial to creating a sustainable model. Anything less invites the kind of backlash we see in adblocking. We note here the point the Commission made in the interim report that by and large Australians are trusting of the institutions holding their data – particularly the Government. Let's keep it that way.

Four Issues for Consideration

Issue #1 Data Access Won't Always Deliver Data Use

We would point out here that the issues of under use of existing data sets are nothing to do with data access. As analytics practitioners, we see the issues over and over again. Our estimate is that less than 10% of the value of existing data is being extracted currently. And while we see issues of data access as significant, and devote the rest of this response to them, we would be remiss if we did not point out the elephant in the room. Data access is necessary but by no means sufficient to achieve the goals of the Inquiry, and arguably, taking a measure of current usage would reveal a suite of organisational issues that in themselves require recommendations.

[8] https://medium.com/@dsearls/the-castle-doctrine-45c9abc147e8#.p8yfxt2wk

The risk in the Productivity Commission process is that the Commissioners receive input from the converted, and not from those sitting on large piles of data who are not using them. A classic selection bias!

We could go write a book on the subject (and have) but while the issues are to some degree addressed by competition in the private sector (to the extent that the relevant sectors in the economy are highly competitive – another matter), there remains how to encourage the public sector to move forward. The issues here are of organisational inertia in the use of data which might hold the potential to increase efficiency, but create personal risk for decision makers (their jobs and careers are built on old style practices not data oriented ones).

We would urge the Commissioners to consider this and how it might recommend to Government that data use outcomes be implemented in the public service. We note too that the most powerful data for efficiency purposes in the short run is the institutional, aggregated data that poses no risks to individual freedoms and privacy. We would like to see a mantra of "use what you've got properly first".

Issue #2 Data Access Always Creates Risk – So Leaner Data Approaches Are Preferable

As the Commissioners identified, as soon as linked data exists, whether it is identified or not to the individual, there is risk. If the data relates to individuals, the risk is borne by the individual, often unknowingly, and the gain is always to the institution using the data. Two things can redress this notable imbalance because these two forces act against collecting data for its own sake. We definitely need to encourage leaner, safer data practices otherwise we put our community at risk both from data breaches and - more high risk - the unintended consequences of data storage instigated by the agencies trusted with that data. And, secondly, we run the risk of community push back. As the Commissioners have pointed out, Australians exhibit a relatively high level of trust in the institutions around them. Good data practices over decades and arguably lack of community awareness of data breaches that do go on have contributed to public perception. The application of the Privacy By Design principles here go a long way – we examine this in more detail in Issue #4 in our thought experiment on governance of the Comprehensive Right.

Issue #3 – The Risk Asymmetry In Data Use Is Not Going Away – It Needs Pervasive Governance

The Commission's two key pillars - the Comprehensive right and National Interest Data Sets and the management of those rights, we would argue do not go far enough given how all-pervasive data use is. We believe the Commission is well placed to provide recommendations regarding overall data governance for the economy.

Three analogies are provided here which we believe put useful perspectives on the problem but also point the way to established governance models. We do not propose to have the answer but would offer three perspectives in the context of the broader observation that data use has the potential to transform our society similarly to the ways cars have.

1. **Data Access As An Asset (Being A Legal Right Which Can Be Protected)**
   If we think about data through this lens, and the manner with which assets are protected and disputed in society – the full range of supervision/regulation/civil and criminal sanctions are opened up. We believe that this is a fair perspective of data, often call the "new oil" and as such, similarly pervasive controls are required. We do not seek to get in to the issues of who "owns" data. Rather, we suggest that access to and the right to use data is a valuable right which requires protection.

2. **Data Risks Are Similar to Environmental Risks**

   Data and the Environment share some common characteristics in terms of being new constructs seeking to be regulated. The difference, we would argue is that the risk with the Environment is that individual actors gain the benefit of their actions while the risks/costs are borne by society and humanity at large. If you will, the cost/benefits are asymmetric - benefit to the individual, cost to society.

We would argue that data use is almost the reverse. Cost is borne (or at least risk) by the individual, whereas the benefit accrues to organisations. While data misuse doesn't necessarily contaminate the globe in such a clear way as environmental mismanagement, again, there is asymmetry and very significant needs for appropriate checks and balances.

So, our starting position is to ask whether governance for the use of data in Australia could leverage the environmental governance framework. There are laws, oversight bodies, civil and criminal sanctions through to political means of objecting to practices. Further, there are Board requirements for public companies and investor mandates in some cases that require certain levels of environmental management to meet investment criteria.

3. **Public Health Analogies – People's Choices Affect Public Outcomes**

Another analogy would be public health – data safety and management is a task that Australians will have to take more control of over time. The Comprehensive Right gives control to the individual, but if they don't exercise it correctly and individuals experience risk and loss, then the political will to support extended data use might wane. To make sure that the community supports data use to Australia's benefit, there needs to be effort made to supply the context for informed data consents. Children learn about health and water safety. Why not have data literacy as a core element of schooling?

The thinking around this is broadly considered the field of data ethics[10].

Issue #4 Risk Management Does Not Have To Stifle Innovation – It Creates It

The goal of the Inquiry is to enable Australia to make better use of data in a manner that is sustainable. The work on Privacy by Design around the world and the innovations in computing to address awareness of data provenance are innovations that illustrate the potential to have a data economy with controls.

Risk Management Supports Innovation:

Risk if not managed will erode trust and create the wrong context for innovation –right now data innovation is often free riding on existing trust capital.

Taking financial services as an example, it should be noted that banks are in Australia a trusted group of organisations, that trust has been developed over more than a hundred years. When fintech organisations use workarounds because the Comprehensive Right is not in place – impersonating customers using their banking credentials – the result is compromised individual privacy and security. And sectoral risk. The only reason that fintechs can get people to share their banking passwords is in the context that they are sitting within bank processes – so they are free riding on the accumulated trust capital built up by the financial services industry. This is why there is a need to create a sustainable model for data sharing. (Refer Appendix A of Infact Decisions/Verifier Initial Submission).

Data Risk Management Is the Innovation:

The way in which data is collected and transmitted is as much the innovation as the data use itself. We refer back to our prior submission and article in JASSA – not all fintech organisations seek to access data in a way that keeps consumers in control and protected. We note the rise of financial aggregation organisations that

[10] https://techcrunch.com/2016/11/12/data-ethics-the-new-competitive-advantage/

impersonate the customer's banking credentials in order to provide the consumer with access to their own data. This is precisely why an API model or better is required because the counter factual, being the current practice, puts consumers and data sources at risk of being compromised and creates a challenging legal context (note ASIC's two whitepapers on the subject)[11].

Export Potential Enhanced with The Comprehensive Right

The evidence globally, is that the issues around data access and control are front and centre for most jurisdictions where Australian technology companies and financial services companies seek to compete. To the extent that the Australian regulatory environment is in sync with these global changes, the chances are increased that Australian operators will be able to expand globally. We have already seen the issues of meeting data standards in the manner with which the EU General Data Protection Regulation requires adherence regardless of the domicile of service providers who sell to EU citizens.

Case Study – How the Policing Of the Comprehensive Right Ecosystem Might Evolve

In laying the foundation of the Comprehensive Right, the hope is that individuals will take back control of their data and in doing so, will control to their comfort, access and use.

Of course, this is a nascent area. Here we try and pull together in a thought experiment how governance might work for the Comprehensive Right:

Receipts Needed!

In the interviews the point was made that in many ways, the advent of the cash register assisted commerce greatly by creating a cash receipt for both the seller and buyer. This reduced theft (both of staff and customers) and made tax collection far easier for the State. Receipts of transactions created instant transparency – in many developing countries there are fines for not holding on to your receipt. Such is the value of transparency. In the case of data, the Comprehensive Right allows for individuals to access their data. For this there needs to be API or better access (in our opinion). But the Comprehensive Right also includes rights to be notified of sale of data - which therefore needs receipts - and we would argue a right to be notified when your data is linked using "personal" information (probably broader than is currently thought). Again, this right would require receipts.

Help Needed

Once those rights are being exercised (and obligations being kept) we turn to how this will play out for ordinary Australians. We expect they will want help and are fairly sure there will be an ecosystem, by analogy to tax time, where not everyone does their own tax. In many cases, they take their shoebox of receipts to an accountant or tax agent who they pay to do this tiresome work for them. Managing control of data is not a costless activity. We can rightly expect that when this control is handed back to the individual they can and will seek help. This ecosystem is already being built, but regulatory changes will bring incumbents in to the mix and accelerate the process.

Governing The Helpers

So, now let's turn to governance of the helper third parties. They may be start-ups, but there are also definitely going to be incumbents who re-tool. Governance of the Comprehensive Right might include certification of third parties and a default fiduciary duty setting for anyone who handles data on behalf of an individual. If we think about how we regulate doctors, lawyers, banks, airlines, any group who affect the lives of citizens ends up

[11] 2015 REP 426 - http://asic.gov.au/regulatory-resources/find-a-document/reports/rep-426-payday-lenders-and-the-new-small-amount-lending-provisions/, and
2201 CP 20: http://asic.gov.au/regulatory-resources/find-a-document/consultation-papers/cp-20-account-aggregation-in-the-financial-services-sector/)

being regulated at least in the key aspects of their operations where there is risk of individual harm and information asymmetry.

Governing the How – Zero Knowledge Protocols and No Personal Password Sharing

As we have discussed in our prior submission, we suggest that any sensible Governance of the Comprehensive Right would determine that the **how** of accessing data under the Comprehensive Right is just as important as the fact of access. We have already argued using APIs or better. And we point out that impersonation techniques are not OK. AISC has twice raised concerns in Financial Services about password impersonation.. And, the Australia Federal Government has adopted global best practice with its Document Verification Service for online identity. They are one of the few "at scale" examples globally of a zero knowledge protocol. The individual seeking to assert their identity, asserts things only they could know (or a determined thief/fraudster) and the Document Verification Service, having reviewed Federal Government data, returns a Yes/No response. In other words, confirmation is provided by the Federal Government without transmission of knowledge. The popular analogy used globally is the bouncer at a nightclub. You might need to prove you are 18 or 21, but in order to do so you hand over a driver's licence with age, date of birth, height and weight (in some cases) and your address. This is definitely not a zero knowledge approach!

Governing The How – Lean Data – Sufficient For Purpose – Or "Less Is More"

One of the key tenets of the Privacy by Design movement is – keep as little data as possible. A leader in this movement is Dr Ann Cavoukian who is a former Ontario, Canada Information and Privacy Commissioner. She is Executive Director of Ryerson University's Privacy and Big Data Institute.

Principle 2 of Privacy By Design is Privacy By Default – there are four tenets under this principle, of which one is data minimization – the following principles and quote are sourced from a paper by Dr Cavoukian[12]:

- Purpose Specification
- Collection Limitation
- Data Minimization – "the collection of personally identifiable information should be kept to a strict minimum. The design of programs, information and communications technologies, and systems should begin with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized".
- Use, Retention, and Disclosure Limitation

Another useful model is Kim Cameron's Seven Laws of Identity – Kim is Microsoft's Chief Architect of Access and a global thought leader on digital identity[13]. The seven principles are listed here, the first six apply to data seamlessly.

1. User control and consent
2. Minimum disclosure for a constrained use
3. Justifiable parties
4. Directed identity
5. Pluralism of operators and technologies
6. Human integration
7. Consistent Experience Across Contexts

[12] Privacy By Design Principles Reference: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf - a paper written by Dr Ann Cavoukian.

[13] http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

Specific Information Requests – Interim Report

Information Request #1 – Legislative Presumption In Favour Of An Application Programming Interface (API) Or Better

The Benefits

The key benefit of using an API or better presumption is only when that level of connectivity is achieved can the full potential of data be used in business processes. Without this level of data integration, one could have providers use a different format for each of several thousand records. Inconsistent but machine readable formats cannot be efficiently consumed by other systems. Without an agreed translation approach, inefficiencies are created which defeats the goal of enhanced productivity.

There is lots of global discussion about the API Economy – Craig Burton is an author who writes extensively on it and its benefits[14].

Combining API or better access with consumer agency acts as an accelerant to value creation. Still a nascent area, but the assertion we would make is that the value of data in the hands of individuals seeking to transact in the world is far greater than the potential of that same data in the hands of marketers[15]. Currently all the "big data" so lauded is constrained by the inability in many cases for it to be used "in stream". The Project VRM initiative out of Harvard's Berkman Center envisages a model of personal agency that an API or better version of the Comprehensive Right enables[16].
This thinking is mirrored in Europe where concepts of "growth through trust" point to the economic upside that innovative models of enabling data access such as the Comprehensive Right can generate – Ctrl Shift is a UK conference attended by multi sector, large incumbents. This is not fringe, this is becoming, particularly in Europe, mainstream[17].

The Principles

On reflection we believe the key principles are the following - ideally the data is available on demand – relatively instantly (within user experience tolerances), interpretable (consistency, agreed schema), and with the ability for secure delegated access to a third party.

The Costs

The cost of using these principles is that work between organisations in each industry/sector is required to agree common standards. There does not have to be uniformity, but there does have to be consistency. In each industry, there are existing examples of working to such schemas. From credit report in financial services, to airlines bookings systems, through to vin numbers in vehicle related industries.

In Financial Services we see two examples – the New Payments Platform is an industry initiative, whereas the ATO sponsored SuperStream. The issue will be where individuals want access in API or better form and an industry or sponsoring Government agency is not available. This is where a mechanism will be needed.

---

[14] https://www.3scale.net/2014/04/the-five-axioms-of-the-api-economy-axiom-1/; and https://prezi.com/pys_d3ysqbmb/api-economy-update/
[15] http://blogs.harvard.edu/doc/2012/02/13/for-personal-data-use-value-beats-sale-value/
[16] https://cyber.harvard.edu/projectvrm/Main_Page
[17] https://www.ctrl-shift.co.uk/personal-information-economy-2016/

The Need To Be Future Proof

Future proofing is definitely needed hence we would argue to presume a set of principles so as not to lock Australia in to outmoded technology down the track.

Plenty of work is going on in the area of improving on APIs. Examples of needing future proofing abound – one example would be Tim Berners Lee's initiative SOLID[18].

Information Request # 2 – Preconditions for Informed Consent

We would suggest four issues for the Commission's review:

1. Data transparency – the Comprehensive Right if it incorporated notification of **whenever** an individual's data was linked in addition to **mandatory** notification of data breaches would start to elevate data awareness in the community – we note specifically the FDC in the US' recent report on data broking[19].

   Data literacy programmes are necessary to enable consumers to have the appropriate context with which to make informed choices at any point in time – that should be starting in schools.

2. Incentives to design for privacy - the best way to understand what is/is not good consent is to model it. We strongly suggest the Government look to foster innovation and use cases of privacy by design systems, in the public and private sectors via some form of incentivization that encourages incumbents, as well as start ups to start using those principles.

3. Consent needs to be experiential – an example below explains, using the analogy of a card game, what happens with data. There are very rare examples that show what consent looks like viscerally[20].

4. Consent will evolve to person driven terms rather than standard corporate terms. In other words, we contemplate a future of at least some degree of inversion of current practices. Instead of signing up to company terms, companies will in some contexts sign up to those initiated and managed by individuals and their agents. This concept of Customer Commons is an active area of research and development. It is crucial that the Inquiry be aware of this because the point is, consent models are likely to profoundly change at least in some sectors of the economy in the medium term[21].

Information Request # 3 – Individual's Privacy Concerns

Regarding the information request on citizen attitudes to privacy – provided below are some extra examples from overseas where disclosure of data breaches seems to create higher awareness and more concern:

[18] http://www.digitaltrends.com/web/ways-to-decentralize-the-web/ and https://solid.mit.edu/

[19] https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[20] http://digi.me/video

[21] http://customercommons.org/, https://medium.com/@dsearls/time-for-them-to-agree-to-our-terms-263ee87e9f41#.6p9a2ahz6

- In the US the Pew Institute suggests data breach disclosures have led to 86% of Americans surveyed taking steps to mask online behaviour because of concerns re privacy[22]
- EU level research, from the EU Directorate-General for Justice and Consumers[23].
  Press awareness from the UK on the Chinese Government's Citizen Score – highlighting the concerns that data linkage risks are not limited to outside breaches[24].
- We would also refer to the case study of the rise of adblocking behaviour, globally, as pointing to a situation where individuals, when provided with the tools to manage their data sharing, are voting with their feet. What emerges from the surveys cited above is a malaise on the subject, an apathy of feeling violated with no recourse. Adblocking shows when tools are put in the community's control they are willing to do the work to use them, suggesting privacy is far from dead and the concept of a surveillance economy being far from acceptable.

Information Request #4 – De-Identification To Avoid The Comprehensive Right – Risks

We argue that there are clear risks of abuse if de-identifying data can avoid notification obligations. However, if the Commission saw fit to recommend notification of use of personal data to create de-identified data and, as Europe broadened its concept of personally identifying information, then, at least at the outset, this risk and issue would be known. In other words, at least for the first chain in the de-identification process the issue would be known. After that, if governance included a principle of data provenance then it is possible that sales of de-identified data might be disclosed in some form of reporting.

We suggest that an additional right be included in the Comprehensive Right – the right to be notified whenever an individual's personal information is used as the link between disparate data sets – not necessarily a right to opt out broader than the current proposals – but a right to be aware of the practice. Awareness can enable people to make up their own minds about the practice and challenge it through political, civil suit or criminal sanction.

[22] http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

[23] http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf

[24] http://www.bbc.co.uk/news/world-asia-china-34592186

Is CCR different to the generalized case of data sharing in industries?

We follow up here a question posed in the Public Hearings. We would argue that credit data serves a social function beyond providing data to support transactions. Repayment of credit information acts as a reputational mechanism.

And, credit reporting is a special type of reputational mechanism because its closest counterparts are law courts and the police. The interesting aspect of credit reporting is that it is a private sector reputational mechanism whereas most other reputation mechanisms are state controlled – for more on this references from our first submission are useful and specifically Daniel Klein's 1992 paper[25].

As a result of this specific role as a reputation mechanism, we see a role for the Federal Government in encouraging the best possible level of information sharing in credit markets. We would suggest that whenever these special cases exist, they will be considered of national importance and will potentially operate separately to the situation of the National Interest Data Sets.

In the case of CCR, the work is in removing barriers to the creation of the data set itself, rather than its governance. CCR governance is clearly handled within Part IIIA of the Privacy Act. The role of the Inquiry with regards to CCR is to address how to remedy a Government intervention that has not, as yet, yielded the desired outcome.

There may well be other exceptions and contexts where this sort of "encouragement" of creation of new data sets is required, but one thing is certain, with the operation of the National Interest Data sets there will be fewer special cases to deal with.

In Closing

We thank the Commissioners for the opportunity to provide follow up material and wish the team well in the next, crucial three months of activity. This is an inquiry that is both timely and critical and we hope the material included here is of use.

Kind Regards,

Lisa Schutz.

On Behalf of the InFact Decisions and Verifier teams.

[25] Klein D. (1992) "Promise Keeping in the Great Society: A Model of Credit Information Sharing", Economics and Politics 4(2):117 - 136.