SENATE STANDING COMMITTEE ON COMMUNITY AFFAIRS

SENATE INQUIRY – MY HEALTH RECORD SYSTEM

SUBMISSION BY:

Marie Johnson

Managing Director and Chief Digital Officer

Centre for Digital Business Pty Limited ABN: 16 162 122 072

31 August 2018

Background

I am the Managing Director of the Centre for Digital Business, a digital services and artificial intelligence company.

My background includes extensive public and private sector experience in Australia and internationally. This experience covers policy and strategy, major programme delivery; operational service delivery of call centres; web and digital services; face to face client services; large scale technology services; and global innovation.

I was previously the Chief Technology Architect (CTA) for the Australian Health and Human Services Access Card.

I present a somewhat unique perspective as the Access Card CTA across the business case, its connections into the health system, architecture, co-design, health services innovation, and global technology industry.

Further details on my background is provided in the attached summary bio; online at www.centre-for-digital-business.com; and at LinkedIn https://www.linkedin.com/in/mariehjohnson/.

Introduction

As the (former) Chief Technology Architect (CTA) of the Health and Human Services Access Card, I opted-out of the My Health Record on day #1 - here's why.

In summary, all the issues encountered with the My Health Record, were encountered throughout the Access Card program. All the use cases and counter-point arguments were encountered - and these have not been resolved.

The politically designed or influenced model of a centralised database with widespread access at the edge is deeply flawed. This was the Access Card model and is the My Health Record model. Everything else that flows from that flawed model is problematic and unresolvable: legislation; operational performance; privacy; security; informed consumer choice; and highly contested value proposition.

Politically driven or influenced design – in any domain - usually always ends in failure or compromised outcomes. Access Card was terminated on political grounds, notwithstanding alternative architecture models presented and some of which have now been implemented elsewhere.

And for all those who will be horrified, and argue that I am not an advocate of "ehealth", quite the contrary. Kudos to the many great hospitals, medical practices and health entrepreneurs with foresight who are innovating and digitising their services. The centralised My Health Record approach is not a pre-condition for this to occur and this innovative transformation work should continue and accelerate.

What I am advocating, is a complete redesign of the model. The current My Health Record model is not just of questionable value but I believe potentially dangerous – and that is why my husband (with chronic and life threatening health conditions and disability) and I opted out on day #1. I explain this in some detail in this article.

Last December (2017), we co-authored an extensive account from a consumer and innovation perspective, of the flaws of the government's approach to ehealth: *"Abandoned by Government eHealth — Heart Patient Turns to Apple*". [Reference https://medium.com/@mariehjohnson/abandoned-by-government-ehealth-heart-patient-turns-to-apple-317f1e1df251].

With this Access Card perspective which I believe is somewhat unique, I further add my voice to the recent comments of other expert commentators:

The former *Privacy Commissioner Malcolm Crompton* warned of the dangers six years ago. [Reference: https://www.theguardian.com/australia-news/2018/jul/30/my-health-record-former-privacy-head-warned-of-dangers-six-years-ago]

The Australian *Privacy Foundation's Dr Bernard Robertson-Dunn* considers that the biggest privacy risk to your My Health Record is the government. [Reference: https://privacy.org.au/2018/07/24/media-release-the-biggest-privacy-risks-to-your-my-health-record-the-government/]

From the medical profession, *Dr Kerryn Phelps* has expressed her concern about the far reaching potential implications and the need for a Senate Inquiry.

In the article, "*Staying in or opting out: My Health Record goes viral for all the wrong reasons*", [Reference: https://croakey.org/staying-in-or-opting-out-my-health-record-goes-viral-for-all-the-wrong-reasons/]. Dr Ruth Armstrong explains why the greatest risk of the My Health Record, is that the risks themselves are poorly

understood and asks should we be asking doctors how familiar they are about cyber security. (In my view, there is a liability risk.)

And from a surgeon, *Dr Neela Janakiramanan*, who has written a detailed account of her concerns about the My Health Record that go way beyond privacy. The surgeon shares a comprehensive analysis of what's at stake – and why youth and women in particular are at risk. [Reference: https://womensagenda.com.au/uncategorised/a-surgeons-very-real-concerns-about-my-health-record/]

All these concerns were encountered during Access Card. The issue is not a resistance by the health profession to ehealth – the fundamental issue is the centralised database model controlled by government and from which all other issues flow.

"Centralised Database + Broad Access at the Edge Model"

The analysis of the My Health Record risks and issues starts with an understanding of the model – side by side with the Access Card.

The Access Card and My Health Record effectively are of the same model ie a centralised database controlled by government with access by the consumer, a wide range of health professionals and law enforcement. The (then) Howard Government's own Access Card Consumer and Privacy Taskforce headed by Professor Allan Fels, made a dissenting submission to a Senate Committee of this model and the limited protections.

Legislation

Legislation cannot tie the hands of a future government, and this was one of the issues encountered in the Access Card program. One of the deep problems with the Access Card draft legislation – in an attempt to give assurances and protections – was that it stated that the Access Card was not an "identity card" and further, put into the legislation the design and architecture of the Access Card chip and the Access Card system. Feedback through the consultation was strong given the centralised database model: this did not provide sufficient protections and there was great concern that a future government would change this.

In any case, legislation should not define design (effectively legislate design) because this locks in design and technology obsolesce and makes it very difficult for a system to remain resilient and adaptive.

In the same way, any legislative provisions of the My Health Record are insufficient as these can be changed by any future government (or even the current government). The ab initio problem is the "centralised database + wide access at the edge model".

Opt-In…Opt-Out…or Compulsion

Governments use various techniques to encourage participation and the over-riding consideration in a democracy is enabling informed choice by the citizen. We are compelled to pay tax. There was a period in the 1960s and 1970s where Australian males were compulsorily conscripted for military service. People can resist compulsion but there are consequences and people need to be informed of these consequences.

The Access Card was described as opt-in as a pre-condition for a person to be able to receive health and human services benefits. A person could choose not to opt-in, but they wouldn't be able to receive benefits, including health benefits. Commentators at the time described this as in effect a compulsory regime and that many people, including disadvantaged and vulnerable people, would be pressured into opting-in or would opt-in by default without making or being able to make an informed choice about doing so.

So, opting-in or opting-out - or not - is a highly contextual decision requiring information to avoid inadvertent decisions by default.

In the case of the My Health Record, being in an informed position to opt-out even further discriminates against the disadvantaged. Not opting-out means that many people are caught by default, silently captured into participation without informed choice and consent. This raises potential Human Rights questions in relation to people with disability, Indigenous and the vulnerable - as to whether information provided (or not) impacted the ability of disadvantaged groups to make an informed choice.

Further contributing to the confusion about the My Health Record, is the timeframe for opting-out – and the consequences if a person does not opt-out within the opt-out window, thereby being "in", but later chooses to opt-out.

Legislative change to extend the opt-out window does not resolve this situation.

The "centralised database + wide access at the edge model" is the problem and all other problems flow from this.

Most people do not understand or are even aware of the complexity or personal consequences of this model.

Healthcare Scenarios and Use Cases

The Access Card encountered all the same use cases and scenarios as My Health Record is encountering: ambulance paramedics; hospital emergency; moving between doctors; diagnosis support; access by minors; complex family situations; the homeless; people with disability; people being able to add additional information; and so on.

It is now more than 10 years since the cessation of the Access Card, and none of the complexity around these use cases has been resolved. And this is because the root cause problem is the "centralised database + wide access at the edge model".

Before going into some of the privacy and security questions – which other commentators have covered very well – it is worth thinking about the practical operational health delivery implications of reliance on a system based on a "centralised database + wide access at the edge model".

Practical Operational Considerations

During the Access Card program, all the scenarios listed above were also examined from a business process and operational systems performance perspective and the practical implications of these in health delivery.

Detailed in situ business process modelling was done and strong feedback was given by health professionals and practice operators as to the difference between theoretical use cases, however well planned and detailed, and the human experience reality of health service delivery.

It is assumed that the My Health Record program has undertaken similar detailed scenario modelling and business process mapping.

For example, take the use case of a pharmacy transaction involving the presentation of the Access Card: the systems response time between the terminal in the pharmacy to the central Access Card system; the impact on customer service; queues and wait times due to additional processes involved; fall back processes due to Access Card system unavailability; pharmacy staff training and so on. All this presented the prospect of a direct and considerable cost impact on the pharmacy operations.

Similarly, for medical practices, including for example, additional processes for doctors and the time impact in the consulting room; use and access by practice managers and admin staff. Similar mapping was done for emergency situations. Every second or sub-second (if possible) Access Card system response time in every interaction would have added to costs; imposed additional administration and processes in the consulting room; impacted consumer wait times and critical decision making time.

From a scale and operational performance perspective, with a "centralised database + wide access at the edge model", there would be very real challenges in safeguarding the uptime and reliability essential for a nation-wide real time system to sustain health service delivery operations. One might think about air traffic control systems although the difference being air traffic control is a highly regulated and highly redundant network. The My Health Record model however is not a network. The fact that the My Health Record website went down on the first day of the opt-out period – a simple transaction – indicates a critical under-estimation of risk in operational performance.

Privacy

The Access Card program ultimately faced insurmountable challenges in relation to privacy and concerns over function creep, the Senate Committee into the Access Card legislation stated. [Reference: https://www.aph.gov.au/~/media/wopapub/senate/committee/fapa_ctte/completed_inquiries/2004_07/access_card/report/report_pdf.ashx]

> "*3.89…The (Access Card) register gives rise to the prospect of the government having unprecedented access to a single national database containing the majority of Australia's adult population's basic personal information. It is seen as presenting a major risk to personal privacy and security, not only*

> *from government agencies but also other parties with malicious intent. The Fels' Taskforce put the significance of the register into historical perspective:*
>
> *No previous Australian government, even in wartime, has effectively required all citizens to give it a physical representation of themselves, nor contemplated having this stored in one national database."*

More extensive than the Access Card data holdings, the My Health Record centralised database will grow to contain potentially the entire Australian population – adult and minors – not basic information, but health records.

The UK care.data program, the controversial NHS initiative to store all patient data on a single database – equivalent to the Australian My Health Record program – was suspended in 2016 by the UK Government following a review into concerns over privacy, the lack of informed consent, and the sharing of medical data with analytics firms. [Reference: https://theconversation.com/care-data-has-been-scrapped-but-your-health-data-could-still-be-shared-62181]

Similarly, the UK National Identity Card was abolished in 2010 by the UK Government over concerns about privacy and function creep. [Reference: https://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards]

The strategic architecture of the UK National Identity Card and the Australian Health and Human Services Access Card was broadly equivalent, including the "voluntary" nature of both: anyone who applied for UK ID card had their personal details automatically logged on to the UK national identity register.

These four national centralised programs – the Australian My Health Record; the Australian Health and Human Services Access Card program; the UK care.data; and the UK National Identity Card – are all broadly equivalent models.

They are each models of national centralised databases of populations with wide access at the edge.

They all have faltered on privacy grounds; purpose; confused and default consent models; concerns about security; and concerns about function creep.

Security

There has been strong commentary and concerns about the security of the My Health Record "centralised database + wide access at the edge model" with the My Health Record now referred to a Senate Inquiry.

My commentary here is about the security challenges arising from such a model – the same model as the Access Card.

Of course, the cyber security challenges of this model are exponentially greater now than 10 years ago during the Access Card program.

And this will always be the case with this centralised database model. The cyber security challenges over the coming 10 years are almost unimaginable…and the trends are worrying.

And despite this, the Australian Government has persisted with this "centralised database + wide access at the edge model".

The former Pentagon cyber chief, Jonathan Reiber, says hackers could exploit My Health Record flaws. [Reference:https://www.afr.com/technology/former-pentagon-cyber-chief-says-hackers-will-exploit-my-health-record-flaws-20180805-h13lb5]

What has been learned from the experience of the Access Card, from the abandoned UK care.data, and the abandoned UK Identity Card program? All big centralised database models of population data. Why has this model been adopted again? These are serious questions for the Australian public to have answered.

From my experience as the Access Card Chief Technology Architect, the adoption of this model yet again raises a number of mission critical design issues.

A system is only as resilient as its weakest link. Even if "military grade" security applies to the centralised database (described by commentators the during Access Card program as a "honey pot"), securing access at the edge involving some 900,000 individuals in a great variety of environments, is a far greater almost impossible challenge.

The design compromise and risk of the weakest link factor really needs to be understood. It is worth reading the case study of the Space Shuttle Challenger disaster and there are indeed a great many lessons to be drawn from this ranging from governance to risk and decision making involving complex systems.

Two lessons in particular apply for the weakest link risk issue.

Firstly, in the Challenger case, design and manufacture was heavily shaped by political influence and this resulted in the need for O-rings joining sections of the rocket boosters. The O-ring design feature was the weakest link.

The second issue was decision makers ignoring technical advice regarding risk. The night before the Challenger launch, the engineers provided advice to NASA management that the forecast temperature in the morning was for ice and too cold for launch: this would almost certainly cause O-ring failure. The advice was over-ridden by NASA management which proceeded to launch, resulting in the catastrophic loss of the Space Shuttle and crew. The Space Shuttle program was suspended while a review and redesign of the Space Shuttle was undertaken. And this is what I'm advocating for the My Health Record.

The weakest link in the My Health Record model is in fact many: each one of the 900,000 users many times a day in a great variety of environments.

The My Health Record "centralised database + broad access at the edge model" creates privacy and security challenges that are practically unresolvable.

Confused Value Proposition - What the MyHealth Record Is and Is Not

The value proposition of Australia's approach to ehealth has been contentious and confused for decades, as illustrated by the 2011 report from the Parliamentary Library "*The ehealth revolution — easier said than done*." [Reference:https://www.aph.gov.au/about_parliament/parliamentary_departments/parliamentary_library/pubs/rp/rp1112/12rp03]

This Parliamentary Library report referenced comments by Dr David More who was described as *"a strident critic of Australia's eHealth directions for many years*". Whilst his comments were made 6 years ago, the fundamental point of a confused value proposition persist.

> "*A system designed for use by clinical professionals is an utterly different beast to the system that might be designed to help a consumer keep track of their…basic health information and the health story…The bottom line is that creating a system to be used by consumers and clinicians is just a fundamental nonsense. Any system targeting both groups will satisfy neither, inevitably."*

The confused value proposition of the My Health Record is perpetuated by a lack of clear evidenced based communication, supported by all stakeholders, enabling all Australians to make an informed choice.

Administrative efficiency is not a value proposition for consumers. Governments tend to both vague-up and exaggerate this point.

A consumer value proposition is something in the eyes of the consumer – not a marketing claim held out by a government or enterprise. Let's consider two of the claimed consumer benefits.

We are told that the My Health Record is not a complete record: it is a summary of government funded health services transactions, with two year's history initially loaded into the My Health Record.

In written communication in brochures to health consumers, the government states that "…*you don't need to remember and repeat your medical history…*"

Apart from the fact that the My Health Record will not be complete but will be a summary - so people will need to have conversations with their healthcare provider – this gives false assurances to people who are vulnerable and uninformed - that they don't need to repeat conversations about their health status. This approach assumes that these conversations are not valuable and serves to keep the vulnerable uninformed and even more dependent on the state.

In her article "*Staying in or opting out: My Health Record goes viral for all the wrong reasons*", [Reference: https://croakey.org/staying-in-or-opting-out-my-health-record-goes-viral-for-all-the-wrong-reasons/] Dr Ruth Armstrong emphasises to the contrary, the benefit of the conversation and taking an oral history and the importance both clinically and medico-legally.

Would we encourage people not to have updated conversations about their superannuation and financial planning? Would we diminish the value of even having these conversations? To the contrary, people need to be educated, supported and encouraged (not discouraged) to have these conversations with their health providers – without the intervention or brokerage of the government.

As a further indication of the confused value proposition, the My Health Record website states that people can choose to upload other information such as their Advanced Care Plan. Think about this for a moment. At the most traumatising time in life, you or your loved one will log onto a government website to get this precious document. This simply will not happen – that was our family situation last year. This is not a document that government needs to be anywhere near. The Australian Government should not be the controlled holder of the Advanced Care Plans of the Australian population. And it is certainly not a document that 900,000 people should be able to access.

I provide this narrative as I find it very difficult to believe that any co-design was undertaken to demonstrate the "additional benefits" of the My Health Record "centralised database + broad access at the edge model".

The My Health Record is not an "Electronic Health Record". It is not "ehealth" nor "digital health" – these are far more holistic and contemporaneous concepts central to wellness, healthcare and quality of life.

The My Health Record is in effect a "government health record" of you and the government funded health services provided. Furthermore, through this model, the government is effectively mandating access to health records created by commercial organisations such as private hospitals and other allied health professionals, that you pay for, not the government.

The My Health Record is a shell, the purposes for which are not clear, but will inevitably be used for compliance and to monitor and ration the provision of government funded health services.

In closing

It is most appropriate that the Senate Inquiry terms of reference go beyond security to consider the proposed benefits of the My Health Record. The benefits and the risks are functions of the model, and within the scope of the inquiry, I would advocate challenging the presumption of the "centralised database + wide access at the edge model".

The root cause of the privacy, security and other challenges is the very model itself. Based on my insights as the Access Card Chief Technology Architect and other experience across government and globally, I do not believe that any of these challenges can be resolved unless the model itself changes.

I see grave personal and privacy risks inherent in the current My Health Record capability model. And this is the reason that myself and my husband, who has serious life threatening conditions, opted-out on day #1 – and instead choose to use and rely on the Apple health ecosystem. And have done so with full confidence even in serious emergencies.

The Australian public need to be engaged and fully informed about the real and complex risks, and the very purpose of the My Health Record.

Recommendations

- Suspend, review and redesign of the My Health Record initiative.
- Release of any business case to provide traceability from any business case to the current status.

~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~

MARIE JOHNSON

Marie Johnson
Managing Director and
Chief Digital Officer
Centre for Digital Business Pty Ltd

Marie is the Managing Director of the Centre for Digital Business, a digital services and AI company. Within the global digital community, Marie is recognised as an innovator, skilful executive and thought provoking commentator.

Marie conceived and led the global co-design and co-creation effort with people with disability to deliver "Nadia" the first AI digital human for service delivery, which has attracted worldwide interest.

With extensive public and private sector experience in Australia and internationally, Marie has led the strategy and implementation of significant social and economic reforms to the digital machinery of government across service delivery, revenue, identity, payments, immigration and disability services. These initiatives involved multi-jurisdictions, other national governments, and international research, technology and standards organisations.

The diversity of roles covers service delivery operations, global technology strategy, Chief Information Officer, Chief Technology Architect, Technology Authority, board director and advisor, and mentor to start-ups.

The US Government awarded Marie an *O-1 Visa* (Individuals with Extraordinary Ability or Achievement) to take up the role leading *Microsoft's Worldwide Public Services and eGovernment business*, including Microsoft's Identity Strategy in Government. Microsoft noted Marie's egovernment knowledge "…is unique in the world and is of particular interest to Microsoft as we pursue our egovernment strategies".

In addition to large scale service delivery operations, Marie has led the strategy and implementation of significant reform programs across the digital machinery of government:

- ABN registration in joint task force with the ATO.
- The Business Entry Point, initiative of the three levels of government.
- Chief Technology Architect for the $1billion Health and Human Services Access Card programme.
- Initiated and delivered BasicsCard.
- Collaboration with the Reserve Bank of Australia on innovation in payments and information services industry task force.
- Service Delivery Reform technology business cases bringing together Centrelink, Medicare and Child Support.
- Delivery of the $700 million Visa Pricing Transformation (VPT) programme; and delivery of the Global eMedical system to 100 countries in partnership with Citizenship and Immigration Canada at Department of Immigration and Citizenship (DIAC).

The egovernment and digital initiatives Marie has led have been also been recognised globally.

- These include the *United Nations Public Service Award* in the category "Application of ICT in government: egovernment" for the Business Entry Point (www.business.gov.au) which she led for 5 years.
- In 2006-2007, Marie was named "*Innovative CIO of the Year – Australia*".
- In 2013, Marie was named one of Australia's "*100 Women of Influence*".

For many years, Marie was an invited member of the Accenture Global CIO Advisory Council; an Independent Member of the Australian Federal Police Spectrum Programme Board; and an elected National Board Director of the Australian Information Industry Association (AIIA).

Marie is currently a member of the New South Wales Digital Government Advisory Panel; and NZTech.

Qualifications: MBA (Melbourne Business School); Bachelor of Arts; Harvard University Kennedy School of Government Senior Executive Fellows Program; and Graduate of Australian Institute of Company Directors.