From:	digital identity
To:	Brooke McGurk; Dejana Giatras; Michael Sibly
Cc:	Rachel Bateup; Long Tran; Christine Klement
Subject:	[SEC=OFFICIAL] FW: Digital Identity Legislation
Date:	Wednesday, 14 July 2021 10:45:14 AM

OFFICIAL

-----Original Message-----
From: mhaeaking@freeuk.com <mhaeaking@freeuk.com>
Sent: Wednesday, 14 July 2021 06:20
To: digital identity <digitalidentity@dta.gov.au>
Subject: Digital Identity Legislation

May I offer comments on the following topics:

Clarity on the definition of 'Relying Parties' under different models; Transactions that are not covered by contract; The omission of the potential impact on Australians who are not (or not yet) participants;
Recent International developments.

It appears that two very different models are conflated:

The first is where there are various departments and agencies in the public sector that are either planning to go online or already providing services with a common component. In this case it makes good sense for them to have the option to outsource that component in an open, fair and consistent way. Responsibilities and liabilities are clear. Whatever novel aspects online or identity may bring, all could be done under contract (except perhaps with some technical legal detail on State and Commonwealth roles to sort out). In this model the individual is merely an incidental beneficiary.

The second 'user-centric' version is that people need to provide attributes to myriad parties of their choice (except when there is no choice with a monopoly provider such as the public sector). This is so that the other party can do what is required of them to check (and record the checking) under a variety of statues, regulations, or standards. Passports or driving licences are currently used or abused, and there is a sense that this could all be done in a much better way online. These relying parties potentially range from local scout groups or corner shops selling age restricted products to an Indonesian hotel reception, NZ car hire companies, US pornographers, potential employers, and the taxation department as well as future courts, auditors or arbitrators. Whether interceding or providing a 'data wallet', one or more providers or brokers would be handling (and making money from) personal data, much of which comes from official sources. The time-bounded 'service' which they provide has many challenging unfamiliar features (e.g. handwritten signatures do not expire). There are also unbounded liabilities related to the use of the data of victims of ID theft, who are typically not party to any contract but may be damaged financially or reputationally, and there are also new opportunities for fraud and abusive control. In this model market dynamics do not work if the choices are not being made by the party paying. For a contract the 'consideration' need to be identified.
Businesses and charities need to be able to estimate what compliance will cost.

It is hard to disentangle where the proposal is in between these two extremes; parts which make good sense at one end are inappropriate for the other, and there may have been aspirational creep.
The idea that Relying parties (RPs) need to be approved but are not accredited participants may or may not be an editorial issue, but anything that a RP should be doing anyway, such as compliance with data protection principles, may be noted in the explanation and design, but enforcement falls elsewhere. The individual ought to be able to
ascertain, to their satisfaction, who the RP is. The need to provide

for relying parties who are necessarily currently unknown does not sit easily with the outline charging regime. In model 2 it does not make sense for RPs in general to need prior approval.

Some transactions between the public and private sectors are not a matter of contract. As with fraud, they are treated using criminal law and standards of proof, for which lower levels of assurance may be inappropriate, especially when combined with any reversal of the burden of proof.

Assuming that issuance will have about the same fraud rate as passports, and that Australia is reasonably good by international standards, it can be expected to be around 1%. Victims of identity hijack are likely to be those people who, for whatever reason, have not yet become users. They – and there could soon be hundreds of thousands of them with newsworthy sob-stories - have been wronged, but may not know for a long time; this has been facilitated by the issuance of credentials by some party to the wrong person. The proposed evaporation of liability seems to be based on the idea that a bus driver is not responsible for passengers transporting stolen goods. But where an IDP is making money from processing personal data, they would clearly be using it without the individual victim's knowledge or consent. It seems to be saying that some standards will be set and, so long as the relevant one is followed, the victim has no recourse against the relying party nor the identity provider, nor the setter of the standard. Repair of errors must be possible, and putting the cost and onus on the victims is surprising as well as questionable public relations. If the system is 'blinded' then the relying party will be unable to identify the said party, and, conversely, the issuer will have no record of all the others to whom it now knows it made an erroneous assertion.

The real person who finds from a relying party that some transaction has been done in their name will typically have the utmost trouble even establishing that they were not aware of the account, to which they will be unable to log in; yet any repudiation will need to be checked to avoid users disclaiming their actions.

(Consent cannot plausibly be the legal basis for the checks during initial enrolment since by definition it not yet established that it is the claimed person. It would also be odd for it to be a consideration in preparing and presenting evidence, and it's not appropriate in fraud
prevention.)

Earlier this year there was a Swiss plebiscite which overturned a law introducing private sector IDPs; it obtained a majority in every Canton.
Australian voters may well have different views on the roles and responsibilities of the public sector, but may still be uncomfortable about someone making money out of their 'identity data' with no public-sector-only option. But if that's good, why expect plenty of people to use something else?

For long-term commitment, it is prudent to have at least support in principle from the Opposition to avoid the waste of investment experienced in the UK when the ID card and associated population register were scrapped without compensation - in line with the manifesto of the incoming regime.
The move to online services in the UK has resulted in a very significant increase in fraud, and an independent analysis exploring whether the envisaged fraud reduction will be outweighed by new fraud opportunities should be part of the impact assessment for the proposal.

The EU's own review on eIDAS concluded that it had not delivered the expected results, and it would be instructive to consider the overlap with what is proposed in Australia, despite the many differences in law, structure, and registers. Note also that using the law as a project management tool precludes agility. The proposed new EU approach calls for a consistent provision for 'high' assurance to avoid merely transferring the excluded to being second-class 'citizens'. It also continues to preclude demanding anything higher as that would form a barrier to trade.

Mark King