Chris Drake
CryptoPhoto.com Pty Ltd.
PO Box 988,
Noosa Heads, QLD, 4567

20th October 2017

Submission to the 2017 digital economy strategy consultation.

My name is Chris Drake. I am a computer security professional and expert with 35 years cyber experience, I have won numerous international cyber security and innovation awards, spoken at many international conferences on the subject of cyber security, I run multiple security-related businesses, and I own several security patents, including the world's #1 most-cited cyber security patent of all time. I have been closely involved with numerous recent government digital delivery services, in at least the following roles: tenderer, participant, user, observer, and reporter of security oversights. I travel regularly to government events relating to digital delivery and cyber security both within and outside Australia, and I am member and active participant in several working groups relating to security and digital service delivery.

My submission relates to one of the most important topics of the digital economy: security and identity.

Australian Government needs to **engage industry** to deliver a globally acceptable, true-digital-identity mechanism, and in particular, it needs to halt its existing efforts in the area of the Trusted Digital Identity Framework (TDIF). The internet is global – we need global identity, and it needs to be free from Government constraints to enjoy global adoption.

The technology and protocols already exist today to verify then grant individuals (not just Australians) their own, un-sharable, un-stealable, non-duplicative secure identities, and for individuals to exercise their identities with strong privacy and safety. The benefit of a globally acceptable digital identity standard, built to be secure and privacy-respectful, is the potential for the near-complete eradication of fraud, both online and off.

For example: when monetary payments require an identity to accept them, it prevents criminals from anonymously profiting from their crime. When software updates require authors to sign them, it prevents malicious actors injecting flaws or viruses. When online sellers defraud buyers, they damage their own reputations in the process, preventing future buyers from fraud. When email senders sign their communications, spam is rapidly eradicated. When you receive a phone call from a stranger claiming to be someone, or work for some company, you can say "prove it" to receive instant verification (or if it's a scam caller, instantly know it's a scam, and blacklist the scammer from attacking other victims as well). When a website wants to block people from getting more than one account, or wants to exclude known troublemakers, or prevent robots, it can request permission from you to check any of those things (in a way that is both safe and secure). When you log in to websites on the internet, or telephone companies or government, or meet businesses or people in person, modern digital identity makes it possible to easily prove "who" you are, and know for certain "who" the other party is (and that it's not a scammer or impersonation). More importantly, you never really need to prove "who" you are to anyone, and modern digital identity allows this too. A pub does not need to know who you are, but it does need to know you're old enough to drink. You don't need to know who a business receptionist is, but you do need to know they work for the company you're visiting. You don't need to know who a phone caller is, but if they claim to be from the tax office, you do need to know that's true. This is the beauty of modern digital identity. It makes it possible for anyone to reliably know anything they need, and only what they need, to facilitate everyday modern life.

I am a digital identity expert with strong cryptography and security experience. We are at the unique moment in history when it is possible for one country to "spark" the future global identity ecosystem, but to do this, it needs to engage industry experts to build it, and Government itself needs to commit to adopting the solution.

The key to global identity success will be strong privacy protection (without this, European legislation alone would kill it) and zero-risk for authority participants (without which, important institutions will be too afraid to join). Both of these key aspects have become recently technically possible with modern technology and protocols. For example: there is no need for someone who pays money to me to know my identity, however, there may be a need for that person to know if I have been implicated in payment scams or not. This is made technically simple by the introduction of consent-based attestation: when a buyer wants to know if I am a scammer or not, they (or the payment system they're using) can query a reputation service, which requests for me to consent (which I can decline) to releasing to the buyer an indication of my reputation. They can choose not to buy if I do not (or cannot) allow them to check I'm not a scammer. In this way, everyone's privacy is protected while scammers are prevented from perpetrating their craft, and the reputation service bears no risk or liability, because they do not release any information about any party – they merely confirm, or choose to "neither confirm nor deny", the sellers' assertion that the seller is not a scammer. Only the parties to identity transactions release information, never the system, which eradicates liability, and enforces the strongest privacy. In serious situations, court orders may still be served on providers to identify truly evil participants (e.g. terrorists), so this strong privacy does not impede safety or policing (on the contrary, it vastly improves it, since identities of parties is easily discoverable under legitimate judicial process).

The value of an accepted global identity solution is in the hundreds of billions of dollars to the owners, as well as reducing fraud globally by an even larger amount, and facilitating new business processes worth incalculably more. The following is a partial list of some recent Government failures in the identity space, included here to help strengthen the argument that it is time for Government and the DTA (who refuse to engage with Industry) to step aside from Identity-Development efforts, and pass this critically important task on for Industry to .

- Business Authentication Framework (2002): FAILED[1]
- ATO Digital Certificates (2005): FAILED[12]
- AUSkey (2013-2016): FAILED[2,3,4,5] " "inflexible and cumbersome"- *ATO commissioner*. [6]
- ATO Authenticator 2016 (Auskey 4.0?). ATO's most recent security revelations are not encouraging[7]. Plaintext password databases, fake lock-out mechanisms, client-side-only checking, text email recovery…
- MyGov: To the right is their advice about what to do (disable it) when you need their security most (when you're travelling and in cyber-hostile territory) [26] :-

- DTO Digital Identity "Alpha" (2016) – total failure[8].
- DTA Digital Identity "Beta" (2017) – total failure again[9].
- DTA Draft TDIF (Oct 2017) – widely regarded by experts to be unworkable legacy thinking. It is time to dust off the TDIF tender responses, and let the industry experts with already-working solutions put them in place, instead of hiring another team of inexperienced designers to attempt to build such a complex solution?

Yours sincerely
Chris Drake

[1] Source: http://www.itnews.com.au/news/third-time-lucky-for-atos-digital-authentication-176444
[2] Mac: 2013: http://www.smh.com.au/it-pro/security-it/apples-java-block-creates-a-tax-headache-20130211-2e7xe.html
[3] Windows IE: 2014: http://news.softpedia.com/news/Internet-Explorer-Starts-Blocking-Old-Java-Versions-458303.shtml
[4] Chrome: 2015: http://www.ghacks.net/2015/04/15/chrome-42-blocks-java-silverlight-other-plugins-by-default-now/
[5] Everywhere: 2016: http://www.lifehacker.com.au/2016/01/oracle-finally-decides-to-kill-java-plugin-once-and-for-all/
[6] Source: http://blog.cebit.com.au/john-dardo-ato-moving-toward-digitalisation-at-a-fast-pace
[7] Ghastly security record: http://www.zdnet.com/article/the-taxpayer-funded-plain-text-password-store/
[8] In-confidence assessment from state government agency, plus http://www.afr.com/brand/boss/promise-of-digital-government-diverted-by-tech-screwups-20170220-gugpjw
[9] Phone call with interim DTA staff planning a complete restart