



Lockstep Consulting
11 Minnesota Ave
Five Dock NSW 2046
AUSTRALIA

15 September 2019

Department for Digital, Culture, Media and Sport
digital-identity-cfe@culture.gov.uk

Digital Identity: Call for Evidence

Lockstep Consulting thanks the Department for Digital, Culture, Media and Sport for the opportunity to make this submission in response to the Call for Evidence on Digital Identity.

About Lockstep

Lockstep (est. 2003) is an independent research and advisory group, based in Sydney Australia, and dedicated to Digital Identity, privacy and data protection. Lockstep Consulting has been engaged to provide Digital Identity advice and analysis by (among others) the US National Strategy for Trusted Identities in Cyberspace (NSTIC), the Australian Trusted Digital Identity Framework, the Australian Payment Council, the FIDO Alliance, the New South Wales Digital Driver Licence, the National Biometric Matching Capability, the National Authentication Service for Health, the Australian banking industry *Trust Centre*, Identrus, the Open Identity Foundation (OIX), IBM, Infosys, and three American Digital Identity start-ups Confyrm, Queralt and Evernym.

Sister company Lockstep Technologies conducts breakthrough R&D on personal data protection and attributes management. We were contracted over 2016-19 by the U.S. Department of Homeland Security (DHS) to develop a mobile attributes wallet for First Responders. We are the only Australian company to be awarded a DHS identity and privacy R&D grant.

We have a solid understanding of the U.K. digital environment, through our ongoing and widely published global research. We engaged specifically with British local government authorities in 2016 when researching attribute exchange networks for the Open Identity Foundation.¹ We also made a submission to the House of Commons Science and Technology Committee's 2014-15 investigation into biometric data and technologies.²

Personally I have long been involved in public policy for Digital Identity. I was a member of the Australian Law Reform Commission Developing Technology Advisory Subcommittee (2007-08), the National Electronic Authentication Council (1998-2001), the Federal Privacy Commissioner's PKI Reference Group (2000), and the APEC eSecurity

¹ See <https://openidentityexchange.org/blog/2016/11/12/attribute-exchange-networks-new-infrastructure-for-digital-business/>.

² Lockstep's submission was published at <https://bit.ly/2mgoIkj> (PDF).

Task Group (1998-2001). I am currently undertaking a PhD at the Australian Defence Force Academy on the evolution of Digital Identity and its *memetic* attributes, with application to national scale identity infrastructure.

More information is available at <http://lockstep.com.au/about/identity.html> and a broad selection of our research is collected at <http://lockstep.com.au/library.html>.

Our understanding of the Call for Evidence

The Department for Digital, Culture, Media and Sport (DCMS) is working with the Government Digital Service “on the future of digital identity” and has initiated a public call for evidence. DCMS has organised the call into four topics (Needs and problems, Criteria for trust, Role of government, and Role of the private sector) and a total of 21 numbered questions.

Our response provides Lockstep’s considered opinion on the state of free market Digital Identity with reference to your four topics, as well as brief answers to a selection of the 21 questions.

Needs and problems

We face undeniable problems of mounting identity-related crime in digital channels, the apparent ease with which identity information (and personal data in general) can be abused, and terribly inconvenient online authentication and identity proofing. We have faced these same problems globally for well over 10 years, trying to solve them with many public-private initiatives. The United Kingdom’s domestic initiatives have numerous parallels internationally, including the Australian federal government-funded Internet Industry Association authentication hub (2005), the Australian banking sector’s Trust Centre (2007) and the US National Strategy for Trusted Identities in Cyberspace (2009-2017). The Murray Report into Australia’s financial services sector (2014) re-prosecuted the case for a national approach to Digital Identity; since then the Digital Transformation Agency and the Australian Payments Council have worked on public and private sector identity frameworks respectively. A similar vision of a contestable market for Digital Identity services has been pursued for over a decade in Canada and New Zealand.

The unwavering enthusiasm of Five Eyes Nations for a market-driven identity ecosystem seems somewhat unreal when experience shows so clearly that Federated Identity is easier said than done.³ No free market Digital Identity offerings have so far proved sustainable; Canada’s *Concierge* system is well regarded for its credentials being reusable across banking and government, but the system has not yet proven itself beyond the founding cohort and we therefore can’t consider it to be “open”.

³ See also my presentation to the AusCERT 2011 conference, *Identities Evolve: Why Federated Identity is Easier Said than Done* and the published paper at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2163241. In 2013, at the Cloud Identity Summit in Napa Valley, I debated David Rennie of the GDS, who argued that digital identity was “easier done than said”, a position which has not been borne out.

There are a few notable international successes in federated identity but overwhelmingly they have been enabled by legislation; examples include BankID in Scandinavia, and the Estonian national ID card. Lockstep suggests that the lessons of these European programs is almost completely academic for the Five Eyes Nations since they don't have the legislative appetite.

Evidence suggests therefore that the identity problem can and should be reframed.

There is a worldwide trend in the Identity and Access Management (IDAM) industry away from universal identification and towards digitising *verifiable claims*, or *attributes*. Efforts include:

- The *FIDO Alliance* (<https://fidoalliance.org>) is developing technical protocols for authenticating users and mobile devices with reduced reliance on passwords. FIDO is the most important IDAM alliance the world has ever seen, yet it has expressly stated its mission is *not* identification, which FIDO sees as a localised matter for businesses, beyond technological standardisation.
- The *Verifiable Claims* working group of the World Wide Web Consortium (W3C) works on protocols for expressing and exchanging dependable claims about users, such as qualifications, account details, roles and so on.

Andrew Nash, former Product Director of Identity at Google and now Vice President of Consumer Identity at Capital One, put it simply at the Cloud Identity Summit in 2014: "attributes are more interesting than identity".

Lockstep concludes that "identity" remains too loose a concept to translate smoothly from the analogue real world into the digital domain. We also note that fear and loathing of a national ID is inevitable, understandable, and distracting to the Digital Identity mission. We therefore suggest that a pragmatic, theoretically robust and politically lower risk approach is to reframe the identity problem.

The root technical problem online is this: *The things we need to know about people or entities in order to deal with them are difficult to know with certainty in the digital environment.* Commerce and government services revolve around established facts and figures of end users (i.e. attributes) such as account numbers, government IDs, customer reference numbers, employee numbers, professional qualifications, memberships, company positions, social security entitlements, driver license numbers, and personal attributes, like age, marriage status, residency and health conditions. All these critical pieces of identity information and other personal data lose their reliability and *provenance* online: we cannot tell where the information is supposed to have come from, much less can we distinguish copies from "originals" (indeed, the concept of originality is all but lost online). Nor can we be sure that data presented online truly belongs to particular individuals, and has been presented when applicable with consent.

Criteria for trust

The Call for Evidence suggests that "[at] the heart of a successful approach to digital identity is the need to improve trust between the person or organisation aiming to prove something about themselves, and the [relying party]". Lockstep respectfully disagrees,

insofar as it would be more than enough in the current climate for us to *simply replicate in the digital domain the level of trust that we are accustomed to* when subjects and relying parties deal with one another in the real world. As we outline above, the priority task should be to obtain reliable information about transacting parties in the digital environment. We suggest that framing Digital Identity efforts in terms of “trust” has tended to overload and complicate the task at hand.

We do not believe that “trust” per se should be an objective of Digital Identity systems, because trustworthiness is an emergent property with just as many regulatory and governmental determinants as technological ones. If we did better at reliably conveying the precise attributes we need to know about one another, then trustworthiness would follow.

Lockstep does acknowledge a trust deficit which needs careful attention at the government, corporate and institutional levels. In our “Post Snowden World” governments seeking to build Digital Identity solutions are under greater pressure to avoid intruding into citizens’ affairs, and, moreover, *to be seen to avoid intruding*. The more complex and novel the proposed “trust frameworks”, the harder it is to convince laypeople that the frameworks themselves are trustworthy. Purportedly privacy enhancing constructs such as “Triple Blind Privacy” have a distinct downside in that they upend the way relying parties judge the reliability of a credential’s source, which complicates liability and legal certainty.

Lockstep argues that the world abounds with sources of truth. We have institutions, businesses, brokers and processes which provide a great many personal and professional attributes which are widely relied upon across the economy. If government focused on improving the way these sources of truth are digitised, without imposing inordinate changes to real world processes, then you would go a long way to fixing the most urgent identity problems.

Addressing specific questions

Here we provide brief responses to selected questions from the Call for Evidence.

<p><i>1. Do you think digital identity checking will be a way to help meet the common needs of individuals and organisations referenced above? What other ideas or options would help?</i></p>	<p>We would like to see a change of emphasis from “identity checking” to “attribute [or claims] checking”. All stakeholders agree that absolute identification should be avoided wherever possible when undertaking routine transactions. The language of “identity checking” unavoidably overloads the task at hand. The words we use matter, and by shifting attention from generalised “digital identity system” to infrastructure for checking concrete attributes, we should see more precisely conceived and designed systems.</p>
---	--

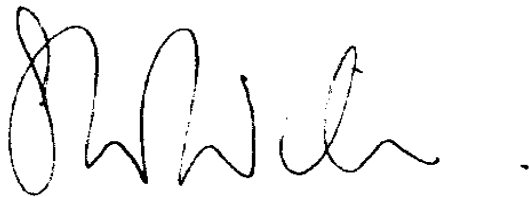
<p>4. How should we ensure inclusion, especially for individuals with thin files?</p>	<p>The thin file problem is complex and calls for flexible, practical processes in the field. On a case-by-case basis, the bona fides of such individuals need to be built up in response to their particular needs for identity-dependent services. Establishing entitlements is first and foremost a <i>social</i> challenge, not a technological one. We suggest that getting thin file cases onto a digital footing must be about verifying and then digitising precise attributes, rather than issuing a new “Digital Identity” as such. For instance, some people will need their medical needs substantiated as a priority, while others, their immigration status and family ties will be more important. There will be no one-size-fits-all basket of personal attributes, and no universal standard for identifying these individuals; that is, it is not clear that there is a well-defined “fat file” for them to aspire to. To suggest that thin file individuals will be granted a generic Digital Identity could have unintended consequences.</p>
<p>6. Where do you see opportunities for a reusable digital identity to add value to services?</p>	<p>In cultures such as Britain’s, with no history of or appetite for national ID, the very abstraction of a reusable Digital Identity (in the singular) is problematic. This might be an unpopular opinion but we do not see opportunity for reusable “identity” <i>per se</i>, because indexing individuals in a uniform way at scale is inevitably going to border on national ID. Instead we urge a shift in focus to <i>reusable personal attributes</i> (or <i>verified claims</i>). There is clearly a need—and in some cases fresh legislative support—for verified digital attributes such as proof of age, address, residency, social security entitlements, health conditions, vaccinations, and so on. Note that some of these attributes are not identifying—and definitely must be conveyable without identification—which reinforces the point that attributes are a more fruitful pursuit than “identity”. We believe that identity is rather over-done, and it would be more powerful (and at the same time less contentious) to assure the provenance and fidelity of specific personal data items, such as those listed, without calling out “identity”.</p>
<p>7. What are the building blocks essential to creating this trust?</p>	<p>Technical building blocks are emerging nicely, as noted above, including the Verified Claims protocols of W3C. In Australia and the U.S., services to verify government credentials such as driver licences and birth certificates are being rolled out. Thus a marketplace of reliable attributes is emerging already.</p>

<p>8. How does assurance and certification help build trust?</p>	<p>Standards, conformance and certification are cornerstones of all commerce, from rail, road and container shipping, through safe electricity supply, to product testing and import/export approvals. Note too that the world has well established Mutual Recognition Arrangements (MRAs) that ensure standards certifications are equivalent across jurisdictions. The trick with Digital Identity attributes is the level at which standardization is really useful. Different business sectors (think of accounting and medicine) have their own well-established processes for credentialing, which are trusted across the board, without relying parties delving into how “identification” is done in different places. In the real world, it is not necessary to standardise identification between accountants and doctors. When digitizing and certifying credentials, it is essential that existing “black box” business processes are, for the most part, left intact.</p>
<p>9. How do we ensure an approach that protects the privacy of users, and is able to cover a range of technologies and respond appropriately to innovation (such as biometrics)?</p>	<p>The bedrock of privacy is Collection Limitation. A problematic side-effect of general-purpose Digital Identity can be over-collection. If a business application requires just one specific attribute, such as proof of age, proof of vaccination or proof of residency, then authentication systems should avoid “identity” as far as possible.</p> <p>Lockstep cautions that biometrics are often a distraction in Digital Identity discussions. Best practice for biometrics in e-commerce is for device unlocking, in a <i>one-to-one verification</i> mode (as opposed to <i>one-to-many identification</i>). The only identification mode which works at scale with current technology is face recognition for border control applications, where lighting and presentation conditions are tightly controlled. Selfie authentication—where a consumer captures an image of their face and photo ID and sends them to a matching service—has become a common pattern only in the past two years. Biometric vendors like to promote their “liveness” (anti-spoof) measures but there is still no independent standard for impersonation resistance. The advent of “Deep Fake” synthetic faces threatens an arms-race where Selfie authentication could be usurped at scale by organised criminals. It’s still early days.</p> <p>For practical reasons, and to minimise consumer anxiety, we urge great care in positioning biometrics in this discussion. It would be premature to cement biometrics in nation-scale Digital Identity frameworks. Government must be clear about what any biometric is for, what mode it will be deployed in, how will its use be constrained.</p>

<p>14. Do you think government should make government documents and/or their associated attributes available in a digital form?</p>	<p>Yes, it is useful for certain attributes to be verifiable over APIs against government sources of truth (as per the experience of the Australian federal government's Document Verification Service, DVS). There is a well-established pattern now for the document checking API to return a simple privacy-preserving "yes/no" answer as to the validity and currency of an attribute.</p> <p>Note that in Lockstep's opinion, the APIs alone are not a complete verification solution. <i>Proof of possession</i> of an attribute is best provided by installing certified (digitally signed) copies of attributes into personal authentication devices, controlled by the legitimate attribute holder, and able to be presented directly to relying parties. See https://www.constellationr.com/blog-news/safety-numbers.</p>
--	---

Thank you once again for this opportunity to engage with the Department's work. We would be pleased to provide more details on any matters raised.

Sincerely



Stephen Wilson
Managing Director
By e-mail.