medConfidential response to the DEA identity SI consultation

This draft SI is entirely unfit for purpose, and should be withdrawn and reset entirely.

We understand what GDS wishes to do, but this is not an acceptable way of doing it as we cover below, which would have been explained to GDS earlier had they not absolutely and explicitly refused to discuss the details with civil society on PCAG or PIAF.

It is impossible to separate the SI from the uses to which it will be put. That HMG may argue otherwise epitomises the mess that this draft exists in – it should never have been put out consultation. HMG should work with civil society (PCAG, PIAF, and any other organisations responding to this consultation who wish to be involved) on a way forward.

Contents

Gov.UK Login

Has Gov.UK Login has metastasized from a "better login to government" project, to a "one identity for government" project?

This consultation is the legislative footing for *exactly* that change.

Unless an intentional policy choice,[1] and unless HMG wishes to attempt to push through this radical transformation of the relationship between citizen and the state,[2] and put highly controversial powers in the state's hands without consultation or adequate consideration, this draft should be entirely withdrawn and rewritten in two halves under the DEA (with a clear primary legislative basis for the database when Parliamentary time allows) to prevent the "big database of the state" being shared across government as lawful under this draft.

A future draft should be shared with all respondents to this consultation, before going, once again, to public consultation. CO/CDDO may wish to examine how this mistake got made, before external questions get asked.

GDS / CDDO should also supply to PCAG and PIAF[3] a paper to be included in the minutes of the relevant meeting on how this SI (and gov.uk One Login) are compliant with the PCAG principles.

---

[1] PCAG has been told no decision has been made, so this should not be the case.
[2] Paragraph 2 https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy-vision-and-scope
[3] and publish in the minutes of the relevant meeting.

Unanswered Questions on the Text

Some of these questions are very general, due to the lack of detail in what has been published. Our response to this consultation remains that the draft should be ripped up and replaced, and that GDS didn't answer these questions in the roundtable, or before we submitted this consultation response shortly before the deadline,[4] shows how poor the work done so far is.

1. This SI comes into force on the day after it is made. Why the rush?[5]

   If the intent of this SI is to build confidence,here is an opportunity to do so in clause 1 in a way which adds no burden to Government. We suggest instead that it comes into effect on a stated, known, date so it can be published and shared between being made and coming into effect.

2. What's Clause 3 (2) (b) doing?

   Clause 3 (2) (b) should be removed, as there has been no justification provided for why it is there, and why "mental health" is a valid purpose, but physical health is not for example. The proposal can not relate to "NHS Login" because that does cover mental health. GDS has failed to explain what this line is *for,* who was consulted on it, and what they said.

3. DEA minutes[6] say that Ministerial agreement has already been sought,[7] so what is the scope for amendment of this Instrument?

   Given how late in the process civil society involvement has been, GDS is faced with no other option than to do another consultation on SIs that can work. The Chief Executive of GDS seems to acknowledge the GDS process failure in a blog stating that there are many questions about the consultation; GDS answered none of them.[8]

General refusal to discuss details with civil society stakeholders

medConfidential asked to see a draft of this Instrument and associated documents prior to the consultation so civil society stakeholders could assist GDS/CDDO in improving the document that went out to consultation. All such requests were repeatedly refused.

GDS shared it to the PCAG-chairs only, but have not allowed them to circulate it more widely. As such, only 2 individuals from PCAG saw the text prior to the consultation, and we do not know what impact that approach had. Hopefully their consultation response will clarify.

We ask a number of questions in this document, questions that should have been answered prior to the consultation open, and remain unanswered 3 days before the consultation closes when this submission had to be submitted.

---

[4] In a meeting, it was said that we shouldn't expect answers prior to the consultation closing, which is a novel choice of transparency by GDS staff. Should GDS choose to provide information they have withheld until the last week of the consultation, we may submit a supplementary consultation response.
[5] Insert usual SLSC/DPRRC references here.
[6] An unclear minute on an opaque process
[7] Item 3.2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1102686/2021-12-07_PSD_RB_Minutes__.odt
[8] https://gds.blog.gov.uk/2023/02/24/helping-more-people-to-prove-their-identity-online/

What's currently seen as missing from the text of the Statutory Instrument

This SI allows any identity information to be shared from and to almost[9] anywhere. The GDS blog[10] suggests otherwise, but the restrictions are entirely current department policy, not legislation. As we see with the missing assessment of compliance with the PCAG principles, policy can change silently.

The SI is not limited to sharing information *with GDS/Login* for identity proofing, nor sharing the defined fields of assured identities with those who wish to rely on those fields.

Bulk sharing is also possible because the SI is not limited to sharing information consequent to an explicit request by the data subject. In practice, GDS wants to do whatever it wants with the complete lack of oversight described above.[11]

4. Why is HMG proposing that this much identity data should be shareable, in bulk, to this many people with this little oversight?

   There must be explicit limits that data may only be shared to CO, and explicit limits on what CO may share to others. Each of those limits should be defined in a new schedule to a new SI (splitting into two SIs will make things a lot clearer).

5. This is an exceptionally broad power, with almost no oversight; far more broad than is remotely acceptable, or those of other powers under DEA. Given the PSD board was not in a position to explore the problems with this text prior to consultation,[12] what gives the public any reason to have any confidence it would resolve future problems?

6. Can Genomic data be explicitly prohibited? It should be.

7. Login will have a great deal of information on users, and the government services they use. As drafted, it looks like that it will all be within scope of the sharing powers. Is that correct? It should be treated identically to any high risk dataset held by Government (ie protected and shared only appropriately, not copied in bulk to anyone who wants it as this SI seems to permit)

8. prior to this draft progressing and being debated in Parliament, it should be made clear in debate with civil society how this proposal interacts with a) the desire to identify veterans and allow them to access the services to which they are entitled, b) HMG's current desire for ID for voting, and c) the identity requirements / obligations around Universal Credit..

The fact that these points need to be *asked* in the public consultation, because they were not answered in the roundtable, have not been answered during the consultation, and medConfidential was not given any opportunity prior to the consultation to ensure there was clarity in the public consultation, shows the flawed process "followed" to get to this point.

---

[9] See the long list of bodies.
[10] https://gds.blog.gov.uk/2023/02/24/helping-more-people-to-prove-their-identity-online/
[11] https://www.whatdotheyknow.com/request/subgroups_of_the_dea_review_boar#incoming-2072525
[12] See minutes

The GDS blog resulting from the chaos says of the SI that “It will enable us to confirm that “yes, this is Jaz Bloggs”, making it easier for Jaz to use the government services they need”, but the Regulation does not say that is the only data sharing method that “will” be used – it could have said that, but HMG didn’t write the regulation to say that. It will also enable a lot of other things.

Liability will sit with GDS?

One of the things that Verify did very clearly was assigned liability, and who did what, and what others could and couldn’t do with that information. Some of the very complex issues were nailed down in contract, so that relying parties knew they could rely on the information shared, because it was clear how it had been created, how it had been verified, and who was responsible if processes hadn’t been followed. Everyone knew exactly where they stood, and what data could and couldn’t be shared, and with whom.

Within the secrecy of the Login programme, it appears that model, and all the benefits that come from it, have been entirely abandoned. This suggests that GDS will be accountable for anything that comes out of the app, even if it thinks it might not be.

If the GDS approach to liability shifting is to simply provide all the details of a verified identity document to any department who asked, they are disclosing that someone is a veteran, that they are a former prisoner, or the nationality of the passport they used to validate their identity, etc, is a necessary part of that, which is of unclear compliance with the data minimisation principle of the Data Protection Act.

For example, a person leaving prison after a decade can not be expected to have a valid passport, or have a valid drivers licence, and no recent credit history; they are an edge case for whom identity assurance can best be done by the area of Government which hopefully did identity checks before releasing the person from jail. Similarly, other areas of state are responsible for care leavers and veterans. However, to deal with those cases without risking disclosure of unnecessary information, and potentially protected characteristics, GDS must be very clear what fields are shared in order to both satisfy these needs, and maintain public confidence..

GDS may have alternate approaches, but since no detail has *ever* been shared by Government on how his is being down, beside the bland and unevidenced statements in the GDS Chief Exec’s blog post, GDS will be bound only by legislation, which is that they can share anything they want, including for “fraud” purposes, as part of burden shifting of liability which, due to the different approach from Verify, remains with GDS for now.

The big database can be shared, so in time, it will be shared

*[13]We started our response to this consultation with an unanswered question: “Has Gov.UK ‘One Login’ metastasized from a “better login to government” project, to a “one identity to government” project?” The answer appears to be yes.

A recent meeting held *during* the consultation was told that the Government intent is to actively prevent individuals from having multiple Login accounts. A person may be able to have multiple email addresses – indeed, they may already do – but Government would attach them to a single “identity”. This regulation allows that database, with email addresses, phone numbers, and identity documents, to be shared in bulk.

***This turns Login into a weapon of the database state that HMG has previously assured many times that it was not building. Were civil society lied to? Or has Cabinet Office changed its position without bothering to tell anyone?**

*In a blog about the consultation, the Chief Exec of GDS says “One Login … is expected to be the first application of the new legislation”, which suggests there will be a second application. It is unclear to what extent DWP embrace one Login for Government for UC, or HMRC’s accountant services, or MoJ’s digital courts, or … Requiring judges or accountants to use their work identity for personal purposes seems an odd thing to do without consulting MoJ/HMRC.

Identities are multi–faceted

*Indeed, many of the civil servants reading this will have a “work phone” as well as their own (personal) phone, and use separate work and home email addresses (as they should). Perhaps, the database state team who would be responsible for sharing under this power should, in their gov.uk email signatures etc, include only their “one verified” email address and phone number. Some users of government services are required by regulatory bodies to use work email addresses, and while the left hand of GDS could require them to route personal use through their work address, the right hand of HMRC/MoJ/etc would tell them not to.

In practice, there will be “many to many” mappings as people are complex (consider an accountant who is also a magistrate and uses their maiden name for some things); GDS will be unable to keep the “one account” promise to departments.

Departments will have to assume that individuals will have the ability to have multiple logins (because they currently do, and will continue to do so), and can manage that if they know; whether GDS also adds burdens on citizens is something they can choose to impose.

Any attempt to deny this is the database state of the most naïve form.

---

[13] If you’ve read our blog post, this text is not identical but has a shared heritage. Paragraphs prefixed with a * are meaningfully different.

This database will *require* people to have a working email *and* phone number

The GDS account creation process requires both a working email address and an active phone number to login. If you are missing either of them, then no access for you – and they have to work to login each time.

*There are many examples in the use of UC where someone is too poor to maintain a mobile phone number, which excludes them from the UC digital service; especially when support services happen to be in cheap offices with very limited mobile phone coverage (we're aware of one support service where staff take the shared mobile phone used for this purpose outside to receive the SMS code, then have to run back inside all the way to the office to type it in before it expires).

*GDS originally chose to require a *UK* phone number for refugees fleeing Ukraine who wanted to *come* to Britain to receive an update by email when the rules changed (since those people by definition were not in the UK, it was blatantly unreasonable to require them to have a *UK* phone number, which GDS refused to accept in private, and only updated the process after questions were asked in Parliament). GDS also required a *UK* phone number for Afghanistan refugees wanting email updates on how to come to the UK, but that group were still excluded in February 2023. The current Government simply didn't care enough to help that group.[14]

HMG reasonably expects everyone to have an account over time, and therefore for this to become a full population database, consisting of verified ID, plus mandatory email and mandatory mobile phone number, whose only statutory basis is this Regulation.

Creating a big database and taking unrestricted powers to share it

To avoid digital disengagement for identity verification, we understand Government are expecting to have an "offline" process, which will store a set of identities to avoid offline revalidation each time, and that this caching would be equivalent to the digital system, which suggests that *all* identity data will be retained by GDS for an unclear period of time.

The surprise, late and incomplete disclosure of this new identity database in Government raises some additional questions about the sharing of the identity information possible under the power being consulted upon:

1. How long will "verified" identity information be held by GDS after verification?
    a. How often will someone with a 10 year passport have to revalidate? Does it change for a driver's licence?
2. *Do services get to determine what recency they choose to accept?

3. For what purposes does GDS currently believe it will use the database it creates?

4. This consultation proposes allowing the entire database to be shared, in bulk, to almost anywhere in Government for any purpose; why?

5. Was anyone outside Government shown this policy before this consultation?

---

[14] We note that GDS has announced, during the period of this consultation, that this restriction is finally being lifted by allowing international numbers to work. It is unclear what this Government expects to do for UK citizens without a mobile phone; this was a missed opportunity to address both for low value services such as "email alerts".

*It appears that GDS simply made the decision for itself, with no informed input or discussion with civil society. That relevant information was withheld until after the consultation had opened reflects how recent engagement with PCAG/PIAF could be considered less than "lipservice". GDS has simply and explicitly refused to provide facts and statements about their decisions, or even the existence of those decisions themselves. It is as if the culture, practices, and ethos of the hostile environment was being applied to Government advisory groups by current project leadership – PCAG/PIAF minutes show those who attend a meeting.

***In some meetings, supposedly informed speakers have demonstrated a clear need to be reminded of the importance of the PCAG principles, and why they're there**, most notably the multiplicity principle where users with multiple identities – such as a work email address and a home email address – may use both without Government requiring them to connect the two. Given the previous paragraph, the consultation response should include an explicit statement by the SRO of the programme that the PCAG principles are being adhered to.

*In a project that could so easily go toxic to public confidence in government digital services, the scope for mistakes, and the neglect for public confidence epitomised by the mishandling of this consultation is deeply concerning.

medConfidential
February 2023