



Digital verification services

– how the government can solve the problem about sex (or else sleepwalk into chaos)

April 2024

Contents

What is the problem?.....	4
Digital verification systems can secure both accuracy and reasonable privacy.....	6
How can the problem be solved?.....	7
Legislation provides for consent.....	7
What should the Secretary of State do?.....	8

The UK government is developing a system for **digital verification services** (DVSs). This has been in development since 2021. When the government invited comment on their plans through a public consultation in 2022, we raised our concerns.¹

The Data Protection and Digital Information Bill² which will establish the regulatory framework for this is now at committee stage in the House of Lords.

Digital verification services are defined in the bill as services provided at the **request of an individual** to:

- (a) **ascertain or verify a fact** about the individual from information provided otherwise than by the individual
- (b) **confirm to another person** that the fact about the individual has been ascertained or verified from information so provided.

The aim of the legislation and the associated “digital identity and attributes trust framework” is to:

“increase trust in and acceptance of digital identities across the UK to help make identity proofing easier, cheaper and more secure and to enable a trusted digital identity market to develop in the UK for those that choose to use it to prove things about themselves, for example when starting a new job or moving house.”

That a person is **male** or **female** is a fact about them that is often important, and that they need to be able to confirm accurately in situations such as registering for a relevant service or job.

The legislation provides for:

- a **trust framework** to be prepared by the Secretary of State
- a **system for registration** of digital verification services providers to be set up
- an **information gateway** to be established, with public authorities having the power to disclose information to a registered verification service provider
- a **trust mark** to be set up for use by registered verification service providers.

The Secretary of State has already published a draft version of the trust framework.³ It sets out how the system will allow individuals to verify that they are who they say they are and that they have specific “attributes”. Attributes are facts (such as address, age, national

¹ Sex Matters (2022). *Sex and digital identities*.

² UK Parliament (2024). *Data Protection and Digital Information Bill (3430)*.

³ UK Government (2023). *UK digital identity and attributes trust framework beta version (0.3)*.

insurance number and qualifications) that may be needed to prove that a user is eligible or entitled to do something. The framework also provides rules that digital verification service providers must meet to qualify to handle the data, to give assurance that it is accurate and secure.

What is the problem?

A key problem with the draft framework is that it states “gender” as an attribute and is not clear what this means. This has not changed through several iterations of the framework (it is now on version 3.0).

Verification of identities and attributes will rely on underlying official records, such as those held by the General Register Office, HM Revenue & Customs, HM Passport Office, National Health Service records and the Driver and Vehicle Licensing Agency (DVLA). But none of these public authorities can currently be relied on to give out reliable (or even consistent) information on anybody’s sex.

The Passport Office will change the sex marker on a passport on request, with a doctor’s note. The National Health Service will issue new NHS numbers with a different sex marker, even for children. The DVLA will change the sex marker on a driving licence on request. None of these requires a gender-recognition certificate. Hence the new digital identity system can incorporate a self-declared, false sex. Unless the problem is solved it is self-ID by the back door.

Accurate information on a person’s sex matters in practical situations, for example:

- **for medical, safeguarding or health risk purposes**
- **to register in a sporting body or competition**
- **to obtain the consent of another person** – for example when a patient has requested to be seen by a female GP, or in any situation where a person might request to know the sex of someone before meeting them, such as dating or having them stay in their home
- **to apply for or undertake a job where being a particular sex is a genuine occupational requirement** (such as a care worker providing personal care for a woman, or a volunteer or staff member in a rape crisis centre)
- **to demonstrate eligibility to use a single-sex service** such as a women’s refuge, a women’s dormitory in a youth hostel, or a women’s changing room at a gym.

Self-identified “gender” is not an alternative to sex in these situations, nor is sex as legally modified with a gender-recognition certificate (this version of whether someone is male or female is relevant only in a few legal situations such as registering a marriage).

The recently published Cass Review highlighted the problem of NHS numbers which are being changed, even for children. Cass found that this prevented traceability of patient records which undermined her research. She also pointed out that it has implications for safeguarding and clinical management as NHS healthcare records become incomplete and inaccurate.

Having unreliable information about a person’s sex or identity is worse than having no information at all.

Allowing people to be misrecorded as the opposite sex in digital identification systems brings with it real risks of harm and liability:

- **People being misdiagnosed or misprescribed and medical risks not being identified.**
- **People being put in unexpected intimate situations** with members of the opposite sex to which they have not consented, creating the risk of discomfort, humiliation, exposure and accidental, or at worst deliberate, assault.
- **People unable or less likely to access services for their sex** (such as cervical and prostate screening services) and maternity benefits because they are recorded with the wrong sex.
- **People gaining access** to opposite-sex services, undermining the privacy and dignity of users and providers of those services.
- **Inability to use official identity to prove eligibility for sport;** misuse of official identity to evade sex-based rules and undermine the fairness and safety of sport.
- **Service providers unable to use digital IDs to develop services because they contain no reliable sex information.**
- **People using self-identification fraudulently for the purpose of accessing, gaining the trust of and exploiting or abusing vulnerable people.**
- **Authorities with safeguarding responsibilities unable to robustly assess risk** related to the sex of children or vulnerable people or the sex of other people.
- **Police and others aiding law enforcement being unable to identify people.**

- **Conflicts and misunderstandings over rules** which relate to sex, and to consent.

These are problems both for people who have transgender identities, and for people who do not.

Digital verification systems can secure both accuracy and reasonable privacy

The current system of recording sex in official records (and allowing it to be changed on an ad-hoc basis) is a mess that was developed without consideration of why sex data needs to be accurate.

The Gender Recognition Act 2004 allows people to obtain a “birth certificate” which shows them as the opposite sex. This act was brought in so that transsexuals did not have to reveal data showing their sex when required to present a birth certificate (such as at the bank) because this was judged (by the European Court of Human Rights) to be a breach of their right to privacy under Article 8. No-one considered how changing someone’s records could impact on the overall coherence of the system for everyone else.

The shift to digital verification services makes this problem acute. But it also opens up an opportunity for a simpler, more coherent and non-medicalised system to provide for data privacy (to meet Article 8) in situations where information is not needed, and accuracy where it is.

A digital verification system has to work for everyone. Building confused categories and inaccurate data into it will mean that there will be no reliable means to record anyone’s sex or to obtain consent to disclose the information. Unless this is sorted out, the logic of the digital identities framework will mean that “sex” cannot be included in the digital verification system at all: if there is no means to say whether a service provider’s information is accurate or not under the trust framework, they will not be able to provide it at all.

It is critical that the problem with sex data is solved before the Digital Verification Service Trust framework is finalised.

How can the problem be solved?

The shift from paper certificates to digital verification services provides both the opportunity, and the imperative for the government to solve the problem caused by decades of ad-hoc and policy-driven misrecording of sex data.

Computer systems demand clear answers, and digital systems allow for privacy about particular attributes in particular situations, much more simply than analogue ones, since only the specific information that is needed in any particular situation is shared, with the consent of the individual.

To avoid chaos and grasp opportunity the government needs to recognise the need for accurate sex data, and **write this into the trust framework**, drawing on the underlying principles that information should be recorded accurately, in clear categories, and only shared with consent.

Legislation provides for consent

Consent is baked into the design of the digital verification system: each time a service provider accesses a person's data it will have obtained consent from that person for specific attributes to be disclosed.

A data subject will only be asked to include the sex attribute in their request only if this is a piece of information the data user needs to know. A person who does not want to disclose their sex in that situation can choose not to use the service.

This is provided for in Section 74 of the Data Protection and Digital Information Bill,⁴ which gives public authorities powers to disclose information related to an individual where the individual makes the request:

- (1) This section applies where—
 - (a) a person is registered in the DVS register, and
 - (b) an individual makes a request to the person for the provision of digital verification services in respect of which the person is registered
- (2) A public authority may disclose to the person information relating to the individual for the purpose of enabling the person to provide the digital verification services for the individual.
- (3) A disclosure of information under this section does not breach

⁴ UK Parliament (2024). *Data Protection and Digital Information Bill (3430)*.

- (a) any obligation of confidence owed by the public authority making the disclosure,
- (b) any other restriction on the disclosure of information (however imposed).

The service provider is allowed (and obliged by data protection law) to provide accurate information about a person's sex, because that is what the person has explicitly given consent for. The service provider can verify that this information is accurate, and then it can be relied on by others.

For example: A woman consenting to disclose the data that she is female to a healthcare provider is consenting to share the accurate data that she is female. This cannot be communicated if the "F" attribute is defined so that it might also be used for a trans-identifying male. A single attribute cannot play the dual role of accurately recording and communicating sex and also validating a person's feelings about their non-sex-based identity. These are incompatible goals for a single binary data field.

The system provided for by the Data Protection and Digital Information Bill is designed for a digital world. The Gender Recognition Act (GRA) was designed for an analogue world. It allowed the Registrar General to issue a new (and inaccurate) "birth certificate" to persons with a gender-recognition certificate (GRC) to avoid revealing their sex in situations where they did not want to. Digital Verification Systems do away with this need.

The GRA does not state that the Registrar General (who keeps a person's accurate birth record even if they get a GRC) must provide inaccurate digital data following a request with consent for data on a person's sex. Section 74 of the Bill makes clear that this disclosure is lawful. A digital identity service provider that has a person's consent to verify information on their sex is not bound by Section 22 of the Gender Recognition Act (which makes it a criminal offence for a person who has acquired information about the actual sex of someone with a GRC to disclose that information).

What should the Secretary of State do?

Digital identity verification systems can solve the problem of confusion and corruption of sex data, but only if the civil servants who design the system are directed that it is a policy goal that the system enables everyone to accurately verify and confirm their sex to others (just like this is the goal for all other attributes).

Without this clear policy direction, they are vulnerable to being driven by ideological convictions about gender identity, and misunderstandings about discrimination and equality.

In fact it would be gender reassignment discrimination if trans-identifying people were not able to verify their sex where the information is needed. It would also be indirect sex discrimination if the system was built so that it could not verify sex data accurately for anyone, since this is particularly detrimental to women.

The Secretary of State should make this clear and set the Department for Science, Innovation & Technology to produce a standard on the “sex” attribute to be included in the next version of the trust framework. The standard would make clear what sex means, and how service providers can verify someone’s sex (such as by reference to their sex as registered at birth, or as vouched by a medical professional).

This work is licensed under the Creative Commons Attribution 4.0 International License.

Sex Matters is a charitable incorporated organisation
(previously a not-for-profit company number 12974690)

Charity number: 1207701

Registered office: 63/66 Hatton Garden, Fifth Floor Suite 23, London, EC1N 8LE

Published 12th April 2024