Digital ID and Informed Consent

What is Informed Consent?

Informed consent is a voluntary agreement to participate in a process, system, or activity after being provided with clear, comprehensive and understandable information about its nature, purpose, benefits, risks and implications. It requires that the individual has the capacity to understand the information, is free from coercion, and can decide based on their own values and preferences. Informed consent is a fundamental principle that applies far beyond medical choices or procedures — it is a cornerstone of ethical decision-making in many aspects of everyday life, because it is about empowering individuals to make voluntary, well informed decisions. Informed consent therefore manifests daily in routine interactions, agreements and systems, where individuals must understand and agree to terms, risks or consequences before participating.

In the context of digital ID systems, informed consent involves ensuring individuals understand how their personal data will be collected, stored, used, shared and protected within a digital identity framework. This requires transparency about the system's purpose, potential risks (e.g. privacy breaches, surveillance, or expanded police powers), costs, ownership, funding, and an individual's rights, such as opting out or controlling their data. For digital ID systems, informed consent therefore means that individuals are fully aware of and agree to the terms under which their personal information — such as biometric data (fingerprints, facial recognition), demographic details, and behavioural data — is processed. This includes understanding who controls the system, how it integrates with other services (e.g. financial, healthcare, or government systems), how laws governing data use may change over time, who funds the system, the potential societal and personal impacts, the risks connected to data breaches, redress for the same, and how costly to an individual this would be, and crucially, whether there is an element of coercion involved in them opting into such a system. This is because informed consent must be:

· Voluntary: This means being free from pressure, coercion, or penalties for opting out of digital identity (e.g. exclusion from essential services).

· Informed: Any decision must be based on clear, accessible information about the system's scope, risks, protections, costs, ownership, expanded use and potential legal changes.

· Specific: Limited to the stated purpose of the digital ID system, not a blanket approval for unspecified uses.

· Revocable: A key tenet of informed consent for anything, particularly digital identity systems, is that individuals must have the ability to withdraw consent and have their data, including insights about their behaviour, deleted. Will this be the case?

What People Need to Know Regarding Informed Consent to Digital ID

To give informed consent to a digital ID system, individuals must be provided with comprehensive, transparent, and accessible information. Below is a detailed breakdown of what people need to know:

1. Purpose and Scope of the Digital ID System: What is the digital ID for? Is it for accessing government services, financial transactions, healthcare, voting, or other purposes? Could it lead to being locked out of services or being refused, say, the ability to access a bank account or to enter a store for food shopping? If so, this would be a form of coercion to opt into the system. What specific services or benefits will require the digital ID? Are there alternative ways to access these services without a digital ID, as if not, this will again be a form of coercion? Is participation mandatory or optional, because if the former, yes, it's again coercion? Are there penalties (e.g. exclusion from social benefits) for not participating? Could the scope change over time? Are there plans or possibilities for laws to be amended to expand the system's use (e.g. from service access to surveillance or commercial purposes), and how will individuals be informed of such changes?

2. Data Collection and Storage: What data is collected? Does it include biometrics (e.g. fingerprints, iris scans, facial recognition), personal details (e.g. name, address, date of birth), and/or behavioural data (e.g. transaction and shopping history)? How is the data collected? Is it through registration, apps, or integration with existing systems? Where is the data stored? Is it on centralised servers, decentralised systems, or cloud-based platforms? Who owns and manages the infrastructure, and who then owns the data stored on it? Is it you as the data subject or the institution storing the data? Does that institution have free rein to use that data as "they see fit"? How long is the data retained? Is there a data deletion policy, and how is it enforced if laws change over time to allow extended retention?

3. Data Use and Sharing: How will your data be used? For example, is it for identity verification, tracking, analytics and/or behavioural analysis? Who has access to such data and analytics? Is it Government agencies, private companies, law enforcement, third parties, or all? Are there cross-border data-sharing agreements? Will data be used for purposes beyond the original intent? For example, could it be used for surveillance, profiling, commercial purposes, or expanded police powers? If laws change to permit broader data use, how will individuals be notified, and can they withdraw consent at that point? Could law enforcement gain expanded powers after individuals adopt a digital identity? For example, could police access real-time biometric data, location tracking, or behavioural profiles without a warrant, and what safeguards prevent abuse?

4. Privacy and Security Protections: What security measures are in place? Is there encryption, anonymisation, or other safeguards to prevent unauthorised access or breaches? What are the risks of data breaches? How would a breach impact individuals (e.g. identity theft, financial loss)? How is privacy ensured? Are there laws

or regulations (e.g. GDPR, CCPA) governing the system? Are there independent audits or oversight mechanisms? Could these laws change to weaken privacy protections? What happens in case of a data breach? Is there a notification process and compensation for affected individuals? Would any criminal charges be applied to a data handler for a serious breach, and if not, why not?

5. Rights and Control Over Data: Can individuals access their own data? Is there a way to view, correct, or update information? Can individuals opt out or delete their data? What are the processes and implications for withdrawing consent, especially if laws or system policies change? Are there mechanisms for redress? For example, if data is misused or errors occur, how can individuals seek remedies, and who is the liable party? How long would seeking redress take, and would it cost an individual money to seek redress? If so, what are the likely costs of the same?

6. Risks and Potential Harms: What are the risks of exclusion? Could certain groups (e.g. those without access to technology, those who do not want to use technology, or marginalised communities) be disadvantaged? What are the risks of surveillance? Could the system be used to monitor or control individuals' behaviour? Could it grant law enforcement expanded powers, such as real-time tracking or profiling, now or in the future? What are the risks of discrimination or bias? For example, could biometric systems misidentify certain ethnic groups, or could data be used to profile individuals? What are the societal implications? Could the system lead to increased centralisation of power, loss of personal autonomy, and/or expanded state or corporate control if laws evolve?

7. Governance, Accountability, and Funding: Who operates the digital ID system? Is it a government, private company, or public-private partnership? What are the implementation costs and ongoing running costs of the system and who pays for it? What is the total cost of development, implementation, and maintenance? Is it funded by taxpayers, private companies, international organisations, or a combination? If private entities fund it, do they gain data access or other benefits as a result of their funding? If publicly funded, can individuals opt out of contributing through taxes if they do not wish to participate in the system? What laws or regulations govern the system? Have they been written yet and if so are they enforceable, and do they align with international human rights standards under the ECHR (incorporated into UK law by the Human Rights Act 1998)? Could these laws change to expand data use or police powers? Is there independent oversight? If so, is it by a truly independent body or a quasi-governmental regulator that may lack impartiality? Are there mechanisms to hold operators and government accountable, both criminally and through civil law, for misuse or errors?

8. Accessibility and Inclusivity: Is all the information to make a truly informed consent decision about digital identity accessible to all? Has it been provided en masse to the public in multiple languages, formats (e.g. braille, audio), and at literacy levels suitable for diverse populations? Have the required Gunning principles been applied

correctly to any consultation process about adoption of a digital identity system? Will the digital identity system itself be inclusive? Will it accommodate people without smartphones, internet access, or technical literacy? Are there barriers to enrolment? For example, are there costs to individuals (e.g. fees for registration or devices), documentation requirements, or geographic limitations?

9. Alternatives and Opt-Out Options: Are there non-digital alternatives? Can individuals access services without a digital ID? What are the consequences of opting out? Will individuals lose access to essential services like healthcare, banking, or social benefits if they opt out of having a digital identity, as if so, this represents coercion? Is consent ongoing? For example, can individuals revisit their decision or adjust their participation over time, especially if laws, police powers, or funding arrangements change?

10. Transparency and Communication: How is information about the system being communicated? Is it consultative or commanding, as if the latter this could be coercion? If consultative, is it transparent, truthful, clear, jargon-free, available in multiple formats, and non-coercive? Are there opportunities for public input as per the Gunning principles? Were stakeholders, including marginalised groups, consulted in the system's design? Will updates or changes to the system or the law around digital identity, be communicated be communicated to the public at all relevant times? How will individuals be informed if the system's scope, policies, legal framework, police access, or funding model changes?

Challenges to Achieving Informed Consent for Digital ID

You will see that obtaining informed consent to a digital ID system is an impossible hurdle to get over for those wishing to implement the same. Even with all of the above information, achieving true informed consent for digital ID systems is impossible because:

· Complexity: Technical details about data storage, encryption, governance, legal changes, or funding may be hard for non-experts to understand.

· Power Imbalances: There is a huge power imbalance between those wishing to implement a digital identity system, and those being asked to adopt the same. As such, Governments or corporations may pressure individuals to participate by tying digital ID to essential services, undermining voluntariness leading to coercion or a form of blackmail.

· Lack of Alternatives: If opting out means losing access to critical services, consent will not be voluntary and it will in effect be a totalitarian system – this is

not representative of a free democratic system and as such we would at that point all need to recognise that we live in tyranny.

· Digital Divide: Marginalised groups, such as the elderly, those in poverty, those who do not wish to embrace technology or those without access to technology or education, may struggle to understand or engage with the system.

· Evolving Systems and Laws: Digital ID systems and their governing laws may change over time, making initial consent outdated if new uses, risks, police powers, or funding arrangements emerge. It is unlikely that there would be wide consultation about such changes and therefore no one would be asked for their informed consent to the same. This makes ongoing informed consent unobtainable – a clear breach of rights.

Remember:

Informed consent to a digital ID system is not a checkbox — it is a fundamental safeguard of liberty. True consent demands full transparency: individuals must be given clear, accessible, and exhaustive information about the system's purpose, data usage, risks, rights, costs, funding sources, legal implications, and the potential expansion of surveillance or police powers. People must also retain the unambiguous right to opt out without penalty and maintain full control over their personal data. Anything less is not consent — it is coercion.

And most importantly: informed consent to a digital ID system is impossible. The scope of such a system is fluid, its future applications unknowable, and its legal frameworks subject to quiet expansion. Consequently, people cannot consent freely and knowingly, and as such adoption can never be voluntary. This is why we repeatedly hear the word mandatory when such a system is discussed. When governance mandates or demands compliance without consent, it has ceased to be democratic and has become authoritarian. In such a system, noncompliance is not defiance — it is a moral imperative. It is the firewall against creeping surveillance, against the erosion of autonomy, and against the quiet dismantling of freedom itself.

As true informed consent to digital ID is unattainable, the only principled response to its proposal that you should make is a resounding "No." This is not just for yourself — but for the generations to come. Rejecting digital ID is not an act of defiance; it is a stand for liberty, a shield for privacy, and a commitment to preserving the freedoms that future citizens will depend on.