Dear Committee Secretary,

Here is my feedback regarding the proposed Digital ID bill and legislation.

Digital-ID verification carries a slew of dangers to a democratic society, for now and a future where a government might not be so benevolent. History is replete with examples of a government overreach stifling freedom, innovation and a thriving society. Our ancestors have fought for a more progressive, free and equal society. As technology evolves, we should not open up a path leading to the deterioration of our progress. As life becomes more digital, leaders should recognise the importance of maintaining parallel analog systems that assist with robustly supporting human activity, in times of electronic system failure, maintaining freedoms and preserving access to those not operating in the digital sphere. The prevalence and affinity for books despite their availability in digital form is an example of how we can flourish in having the best of both digital and analog worlds.

The following outline the dangers and folly of digital identification:

Single Point of Failure, data breaches, cybersecurity vulnerabilities and identity theft:
If the digital ID system fails or is compromised, it can disrupt access to essential services and financial transactions. Storing sensitive information in digital ID databases makes them attractive targets for hackers and can lead to large-scale data breaches. Digital ID systems can be vulnerable to cyberattacks, leading to disruptions and potential harm to individuals. If a digital ID system is compromised, it can result in identity theft and financial fraud.

Privacy Invasion, data profiling, inaccurate data, lack of control, biometric risk, access denial:
Digital IDs can lead to invasive data collection and surveillance, as they often require the collection and storage of personal information. Personal data collected for digital IDs can be used to create detailed profiles for marketing and surveillance purposes. Digital IDs may erode anonymity, making it difficult for individuals to engage in private and confidential activities. Errors or outdated information in digital ID databases can lead to problems with verification and access to services. Individuals may have limited control over their digital IDs and the data associated with them. Digital IDs that rely on biometrics can pose risks if biometric data is compromised, as it is difficult to change biometric information once stolen. Incorrectly flagged digital IDs can lead to wrongful denial of essential services, such as healthcare or social benefits.

Centralization, surveillance state, misuse by authorities:
Centralised digital ID systems concentrate power in the hands of a few organisations or governments, raising concerns about abuse of power. Governments can abuse digital ID systems to monitor citizens' activities, stifling civil liberties. Governments or corporations could misuse digital IDs for political or commercial purposes, infringing on individual rights. Dependency on technology, function creep, exclusion, discrimination: Society becomes increasingly reliant on technology, which can be problematic when systems fail or during power outages. Digital IDs originally intended for one purpose can be used for other purposes without consent, leading to mission creep. Not everyone has access to the necessary technology or documentation to

obtain a digital ID, leading to exclusion of marginalised groups. Digital ID systems may inadvertently discriminate against certain groups due to biases in data collection or algorithms.
Cost & legal challenges: Developing and maintaining digital ID systems can be expensive, and these costs may be passed on to individuals. The legal and regulatory framework for digital IDs can be complex and may lead to legal disputes and challenges.