2 December 2021

Digital Identity Systems Trust Framework Bill

Economic Development, Science, and Innovation Committee

Introduction

Who we are and what we stand for

1. InternetNZ's purpose is to help New Zealanders harness the power of the Internet to do good. Our vision is an Internet that is open, secure, and for all New Zealanders. We work to promote the Internet's benefits and uses and protect its potential. We do all this with a cause in mind, that being the Open Internet. In doing this, we act as part of the New Zealand Internet community.

2. We welcome this opportunity to submit on the Digital Identity Services Trust Framework Bill (DITF Bill). We do wish to appear in person to speak to this submission. Please contact us on policy@internetnz.net.nz to arrange this.

We agree building trust is vital for the benefits of digital identity

3. For most New Zealanders, the first experience with a digital identity system will be using the My Vaccine Pass app under the Covid Protection Framework, which started from 2 December 2021, the same day submissions on this Bill closed.

4. Over time these systems will become much more common in everyday life, changing how people access banking, board flights, purchase alcohol, get discharged from hospital, and access welfare services. But few people are expecting this shift.

5. Research commissioned by InternetNZ has found that only 17% of New Zealanders surveyed had heard of digital identity services.[1] We think this low level of awareness will lead to many people being surprised by the way digital identity affects their lives over the next decade.

6. Digital identity systems promise to improve both privacy protection, by giving people more control over how their information is shared, and also efficiency by enabling easier information sharing for organisations. But these promises of privacy and efficiency are sometimes in tension. Assuring the people using a system a high level of privacy, transparency, and control may require design choices that make it less efficient for business purposes. Upholding trust in

[1] InternetNZ, "Internet insights 2020/21" (forthcoming). Question 70 asked 1001 participants "have you heard about the development of 'digital identity' services in New Zealand?", with 78% saying "no", 17% "yes", and 5% "unsure".

the face of this tension will require robust rules and governance for digital identity systems and services.

7. The DITF Bill sets out legal rules to support secure and trusted digital identity services in New Zealand.[2] The Bill's objectives include driving consistency, trust, and efficiency, supporting interoperable digital identity services, offering people more control over personal information, and enabling user-authorised sharing of information.[3]

8. We agree that building trust is vital to the long-term success of digital identity systems in New Zealand. We understand the type of trust needed in terms of both earning community trust and upholding trustworthy standards. If people in the community do not trust a digital system, they will not use it, as we see in broader digital equity issues where a lack of trust remains a key barrier. If a system is not trustworthy, it might achieve a high level of uptake, but it can still have impacts that cause people serious harm.

9. Our submission examines the Bill from this perspective, asking the following question:

   Does the DITF Bill do what is needed to earn community trust and uphold trustworthy standards for digital identity services over time?

Digital identity is not always good for people and participation

10. Identity systems can create barriers and harms as well as opportunities. Looking overseas, we see that the uptake of digital identity systems can harm people and worsen existing barriers to full and equal participation in society.

11. Identity is a core aspect of being a person and participating in social life. Having your identity recognised by national governments and other groups is often required to participate in society and to exercise basic rights. For example, the right to enter or leave your country may depend on having a recognised passport document. Access to social welfare services often depends on having a recognised identity recorded in a birth certificate. International human rights frameworks recognise the fundamental importance of identity to human life. For example, under the Convention on the Rights of the Child, our government must respect the right of children to preserve their identity and also assist in re-establishing identity for children deprived of it.[4]

12. Because identity is so important to people's lives, the uptake of digital identity systems can lead to serious breaches of human rights, whether these are intended or accidental. These harms can include:

    a. **Worsening existing social exclusion**, for example, some young people in New Zealand need help to get a birth certificate before they can

[2] DITF Bill, Explanatory note.
[3] DITF Billl, Explanatory note.
[4] United Nations Convention on the Rights of the Child, Article 8.

access training and other support services.[5] Shifting to digital identity is likely to add another barrier for these people.

b. **Making digital equity gaps worse**. To achieve digital equity, we need to address barriers people face in the areas of motivation, access to connections and devices, digital skills, trust, and capacity.[6] Uptake of digital identity systems may benefit the majority, while meaning people who face these barriers are further excluded from accessing both vital services like banking and broader participation in society.

c. **Creating new digital failure modes**. In 2017, it is estimated that failures in India's Aadhaar digital identity system affected access to food rations for 2 million people, due to failures in biometrics like fingerprints and connectivity issues particularly in remote locations.[7]

d. **Restricting people to categories which do not respect their identity**. For example, a digital identity system in Bangladesh labels Rohingya refugees as "forcibly displaced Myanmar nationals" rather than recognising their ethnic identity. In New Zealand, the My Vaccine Pass app relies on accompanying photo ID such as a drivers' licence, which may have out of date details for a person's name, gender identity, and photograph, which is exclusionary and offensive for many transgender and nonbinary people.[8]

e. **Reinforcing biases and discrimination**, for example the implementation of digital identity in the Dominican Republic contributed to exclusion of Haitian-descended people from renewing government ID.[9] ID and biometric systems like facial recognition can exclude people who look different from the populations they were designed for.[10]

f. **Collecting and sharing data about people that puts them at risk**. Biometric identity data, such as a person's fingerprints, DNA, and facial features, is inherently sensitive, unchangeable, and open to unwanted uses such as profiling people for targeted advertising, or more directly harmful treatment. When the Taliban took power in

[5] Te Puni Kōkiri, Pae Aronui Evaluation: Year One Evaluation Report (August 2020), <https://www.tpk.govt.nz/docs/tpk-pae-aronui-yearonereport-2020.pdf > p 22.

[6] InternetNZ and The Workshop, "Out of the Maze" (2018) <https://report.digitaldivides.nz>.

[7] The Wire. Jharkhand Girl Dies After Family's Ration Denied for No Aadhaar Link, BJP Blames Malaria. October 17, 2017. https://thewire.in/politics/jharkhand-death-aadhaar-ration-card

[8] Melanie Early, "Covid-19: Concerns raised over 'deadnaming' on vaccine passes", Stuff (22 November 2021), <stuff.co.nz>.

[9] Eve Hayes de Kalaf, "How some countries are using digital ID to exclude vulnerable people around the world", Good ID (2021) <good-id.org>.

[10] Mary Cruse, "Built-In Bias: Digital ID and Systemic Racism" Good ID (2 July 2020) <good-id.org>.

2021, there was widespread concern about biometric data in a US-built system being used to target former government officials.[11]

13. These problems are already affecting New Zealanders. The rollout of the My Vaccine Pass system, though clearly an important risk management tool under the Covid Protection Framework, has led to a range of harms and access barriers for people whose needs may not have been considered in the design process.[12]

14. Research by the World Internet Project at AUT has shown that misuse of data by large organisations is one of the main concerns New Zealanders have about participating in digital life.[13]

This Bill is a chance to get it right in New Zealand

15. We support the goals of this Bill, and we want to help improve it. We think that with the right approach to this framework, New Zealand can lead the world in developing digital identity that is trustworthy, efficient, and inclusive of diverse people and communities.

16. Achieving that goal will require learning from overseas experiences, addressing the gaps in the process so far to earn community trust, and developing a framework that can uphold trustworthy standards over time.

Getting it right requires rules that earn and uphold people's trust

17. People talking about the future of digital identity emphasise a shift away from centralised identity services like the passport office or RealMe, to a decentralised ecosystem where many organisations provide identity services, and people can directly control and authorise uses of their information.

18. We too see the promise in enabling community and iwi organisations to operate their own identity services in ways that work for their communities. We want to see beneficial innovation in digital identity. But some of these systems will fail. To make this shift safe and beneficial, we need robust rules to uphold people's trust.

19. We think the DITF Bill leaves some gaps on the goals of earning community trust, and upholding trustworthy standards over time.

20. We highlight these gaps, and our recommendations to repair them, below. In summary, we think it is vital that the Committee consider steps to:

    a. Require broader engagement to earn community trust;

[11] The Guardian (2021). The Taliban are showing us the dangers of personal data falling into the wrong hands. By Emrys Schoemaker. <theguardian.com>.
[12] James Ting-Edwards, "Digital Identity in New Zealand: Technical choices have human impacts", *Stuff* (1 December 2021), <stuff.co.nz>.
[13] World Internet Project New Zealand, "The Internet in New Zealand 2021" (2021) <workresearch.aut.ac.nz>.

b. Build human-centred design into the trust framework;

c. Bolster the independence of the Board and the Authority;

d. Protect against risks from non-accredited providers and services.

Fill the gaps on community engagement

Engagement so far has not adequately included all communities

21. Engagement on digital identity issues has been very uneven, and has offered few opportunities to hear from diverse people and communities in Aotearoa.

22. We have participated in a series of conversations and meetings with officials working on policy for digital identity systems, with interested technologists and businesses through Digital Identity New Zealand, and to a limited extent with people representing communities likely to face barriers and problems from digital identity systems. These have all been good conversations in that the officials, organisations, and people involved all want good outcomes on digital identity. But vital voices have been missing from the conversation.

23. We are extremely concerned that these conversations have left people out. As far as we know, consultation so far has not offered a real opportunity for experts and affected communities to speak to issues of accessibility, digital equity, and potential harms from digital identity systems.

24. To ensure the trust framework earns the trust of all communities, we think it is vital to address this gap in the engagement so far, and find ways to resource meaningful conversations that include these missing voices. Issues of accessibility, digital equity, and potential harms are fundamental both when this framework is created, and over time as it operates.

Require broader engagement as a foundation for trust

25. We think much more and broader engagement is needed to help the trust framework build and retain diverse people's trust. We recommend the Committee:

R1 Request advice from officials on what consultation has been done so far with community groups, including Māori, as well as people in groups likely to face particular challenges in using digital identity, such as children and young people, the disability community, gender minorities, refugees, migrants, ethnic communities, prisoners, and people receiving welfare services.

R2 Amending clause 20 to require that draft rules must be based on consultation with a wider range of people and communities, in particular:

(a) Adding new clause 20(1)(f) to require consultation with the Human Rights Commission;

(b) Adding new clause 20(1)(g) to require consultation with the new disability agency;

(c) Amending clause 20(1)(d) to list groups representing minority communities and groups with an interest in digital equity issues as examples of "people or groups likely to have an interest in the TF rules".

Build human-centred design into the framework

26. A key capacity gap across government, businesses, and communities is expertise in people-centred and participatory design approaches. Resourcing this expertise as part of the trust framework could help to ensure that digital identity systems are developed based on co-design, community participation, and in other ways that respect the diverse needs of different people.

27. We recommend the Committee:

R3 Seek advice from officials on options to build participatory design thinking into the trust framework, including options for resourcing participatory design approaches and kaupapa Māori design thinking as a part of work by the Authority.

R4 Require human-centred and kaupapa Māori design considerations as a factor for the Authority to consider, for example in approving the design of proposed digital identity services.

The Board and Authority must be independent

The Board and Authority should be independent of the executive

28. The Bill proposes to create a Board to make rules governing digital identity systems under the framework, and an Authority to apply those rules to regulate accredited providers and services.

29. Under the Bill's proposed approach, both the Board and the Authority would be hosted within a government department. We think this proposal does not give the Board and the Authority enough independence to build community trust and uphold trustworthy standards for digital identity services. To credibly regulate digital identity services, including those that government agencies wish to provide and participate in, we think the Board and the Authority need a much higher level of independence from the executive.

Bolster the independence of the Authority and the Board

30. The Board will create rules for digital identity systems, including those to be built and operated by government agencies. We think it is vital that the Board

and the Authority are independent from the executive government. We recommend the Committee:

R5 Establish the Board and the Authority as an Independent Crown Entity rather than within a government department.

Services outside the framework may undermine it

An opt-in accreditation framework puts trust at risk

31. As proposed, accreditation and rules under the Bill are opt-in, and do not apply to providers and services who neither seek accreditation nor use a trust mark.

32. We see a real risk that digital identity services will be offered outside the framework, without its governance or rules, in ways that cause harm and create risks to community trust in digital identity services overall. Consumers are unlikely to know about this framework, and to make informed decisions based on it, without both time and extensive communications and practical experience.

33. We think a useful comparison is found in the regulation of financial services and financial advice. The Financial Markets Authority has broad powers to uphold trust in the financial services industry.

Protect against risks from non-accredited activity

34. We think the goals of consistency and trust in the framework require measures to cover non-accredited people and organisations. We recommend the Committee:

R6 Seek advice from officials on minimum standards that should cover all accredited and non-accredited digital identity systems to earn community trust and uphold trustworthy standards over time.

R7 Amend clauses 13 and 14 to limit non-accredited activity to:

(a) An initial transition period of 5 years;

(b) Specific and time-limited exceptions to be granted and overseen by the Authority, revocable in the event of harms or risks arising.

R8 Adding new offence provisions enforceable by the Authority to:

(a) Deter non-accredited activity which undermines the goals of the trust framework during our proposed transition period;

(b) Prohibit non-accredited provision or operation of digital identity services that pose risks to people after our proposed transition period.

Conclusion

35. We think this Bill offers the chance for New Zealand to do digital identity right, by putting in place rules that start from earning community trust, and continue to uphold trustworthy standards over time.

36. We have proposed ways that the Committee can approach this Bill to support the innovative potential of digital identity in a way that upholds these goals. In particular, we think it is important to:

    a. Require broader engagement to earn community trust;

    b. Build human-centred design into the trust framework, including steps to resource expert guidance and evaluation on human-centred design and kaupapa Māori design approaches for digital identity ;

    c. Bolster the independence of the Board and the Authority;

    d. Protect against risks from non-accredited providers and services.

37. We thank the Committee for your consideration, and officials for their work supporting this Bill. We look forward to meeting the Committee to speak to this submission in the new year.

Jodi Anderson	**James Ting-Edwards**	**Laughton Matthews**
Policy Director	Senior Policy Advisor	Senior Advisor, Māori Outcomes

Appendix: Table of recommendations

Require broader engagement as a foundation for trust

38. We think much more and broader engagement is needed to help the trust framework build and retain diverse people's trust. We recommend the Committee:

R1 Request advice from officials on what consultation has been done so far with community groups, including Māori, as well as people in groups likely to face particular challenges in using digital identity, such as the disability community, gender minorities, refugees, migrants, ethnic communities, prisoners, and people receiving welfare services.

R2 Amending clause 20 to require that draft rules must be based on consultation with a wider range of people and communities, in particular:

(d) Adding clause 20(1)(f) to require consultation with the Human Rights Commission;

(e) Adding clause 20(1)(g) to require consultation with the new disability agency;

(f) Amending clause 20(1)(d) to list groups representing minority communities and groups with an interest in digital equity issues as examples of "people or groups likely to have an interest in the TF rules".

Build human-centred design into the framework

39. A key capacity gap across government, businesses, and communities is expertise on people-centred design approaches, which we think is an important perspective on digital identity systems. We recommend the Committee:

R3 Seek advice from officials on options to build participatory design thinking into the trust framework, including options for resourcing participatory design approaches and kaupapa Māori design thinking as a part of work by the Authority.

R4 Require human-centred and kaupapa Māori design considerations as a factor for the Authority to consider, for example in approving the design of proposed digital identity services.

Bolster the independence of the Authority and the Board

40. The Board will create rules for digital identity systems, including those to be built and operated by government agencies. We think it is vital that the Board and the Authority are independent from the executive government. We recommend the Committee:

R5 Establish the Board and the Authority as an Independent Crown Entity rather than within a government department.

Protect against risks from non-accredited activity

41. We think the goals of consistency and trust in the framework require measures to cover non-accredited people and organisations. We recommend the Committee:

R6 Seek advice from officials on minimum standards that should cover all accredited and non-accredited digital identity systems to earn community trust and uphold trustworthy standards over time.

R7 Amend clauses 13 and 14 to limit non-accredited activity to:

(c) An initial transition period of 5 years;

(d) Specific and time-limited exceptions to be granted and overseen by the Authority, revocable in the event of harms or risks arising.

R8 Adding new offence provisions enforceable by the Authority to:

(c) Deter non-accredited activity which undermines the goals of the trust framework during our proposed transition period;

(d) Prohibit non-accredited provision or operation of digital identity services that pose risks to people after our proposed transition period.