PSGR

Physicians & Scientists for Global Responsibility

December 2, 2021

Submission

Digital Identity Services Trust Framework Bill

Submitted to the:

Committee Secretariat
Committee Secretariat
Economic Development, Science and Innovation Committee
Parliament Buildings
Wellington

Address

PO Box 16164
Bethlehem
Tauranga 3147
New Zealand

Email

info@psgr.org.nz

Website

www.psgr.org.nz

Phone

Ph+64 27 505 0808

PSGR would welcome an opportunity to speak to this submission.

Physicians and Scientists for Global Responsibility Charitable Trust (PSGR) work to educate the public on issues of science, medicine, technology (SMT). PSGR work to encourage scientists and physicians to engage in debate on issues of SMT, particularly involving genetics and public and environmental health.

1. The Physicians and Scientists for Global Responsibility welcomes the opportunity to submit to the Digital Identity Services Trust Framework Bill (hereafter Digital Identity Bill or DIB). There is a pressing requirement for the development of secure digital identity platforms that can store private data. However, we submit that the current Bill is premature and many pressing issues concerning law, technology, commerce and ethics remain unresolved.

Contents

2. The preferred government intervention is a governance and compliance regime targeted to the governing of service providers who would supply. The Trust Framework is designed to 'align with trust frameworks in Australia, Canada and the United Kingdom, and is the basis for delivering on the Prime Minister's commitment under the Single Economic Market agenda for mutual recognition of digital identity services with Australia' (July 2, 2020, Department of Internal Affairs).
3. The public have not been provided input into the policy consultation. Transparently, the Cabinet and official's preoccupation with the DIB concerns operation of the governance board and accreditation practicalities rather than the overarching policy or public interest questions of policy.
4. This fails the goal of being people-centred because governance in this respect is narrow and instrumental. 'Governance' as evidenced in the development of related policy is narrowly constructed (instrumental) and concerns the establishment of a governance board or the accreditation team.
5. Policy papers supporting this DIB and the Bill itself focus on reporting systems, and give no indication that any anticipatory regulation will occur to actively prevent harm. It is not evident that these institutions will have adequate powers of scrutiny, and the regulatory teeth, both to anticipate error and malfeasance, and to monitor and analyse the boundaries of risk and prevent harm before the harm has occurred.
6. The supporting policy and the DIB itself are configured to solve a narrow problem. The proposal assumes that trusted providers will be 'trusted' without setting in place overarching aims and values to assist long-term policy and decision-making.

7. Broader assessment of best practice in other jurisdictions outside the Anglo-American world, including considering the European framework, the Scandinavian countries (progress of the Nordic/Baltic e-ID project (NOBID)), and Estonia appears not to have been undertaken.

8. Governance of digital identity is a distinctly socio-technical - human and technical - endeavour. The decision-making that protects the public interest should be informed by values that then inform technical decisions. The DIB should reside inside a larger policy environment that reflects greater norms and values (as a constitutional approach) - that then guides the legislation and the judgments of officials when presented with information (as intelligence).

9. Democratic deliberation ensures that the policy platform and rules in place are more likely to be robust, reduces risk that unanticipated problems will occur, and creates an environment where a novel technology is more likely to be utilised and trusted over the longer term.

10. Democratic deliberation is important for the development of normative frameworks, publicly shared understandings of common terms which are subject to legal interpretation. Legacy approaches, cultural differences, regulatory dynamics and political environments are all institutional properties which impact how important concepts are understood. [1]

11. Digital identity systems can amplify inequalities and produce unjust outcomes. This can occur through the methods of collection, which can produce barriers to disadvantaged groups; and by the potential use of intelligence gathered through information gathering and accumulation.[2] [3]

12. Stewardship requires resourced technological, legal, ethics-based and technical investment to predict and navigate threats. Surveillance and data theft is often invisible and/or silent. It does not involve cutting and pasting, or the leaving of fingerprints.

13. PSGR submit that broader consultation is required in order to provide an overarching governance and constitutional structure in order to ensure the future DIB is 'people-centred'. We do not consider it necessary to fast-track the Bill through Select Committee and quickly achieve Royal Assent.

14. PSGR submits that the DIB does not progress, and instead, adopts and engages in a transparency-based Kiwi version of 'comprehensive engineering', proposed by Delft University ethics and technology researchers:

    'Adequate solutions to systemic problems - especially a pandemic—are always systems solutions, which take into account many technological aspects, human behaviour, values, and norms. Comprehensive engineering is a form of complex systems (dynamics) engineering (complex adaptive systems) accommodating different aspects of socio-technical systems: systems dynamics and complexity, moral, social (legal, institutional, behavioural and economic, cultural) and technical aspects. This is an interdisciplinary and multi-disciplinary approach to engineering, offering comprehensive analyses and future solutions.' [4]

---

[1] Eg. self-sovereign identity. Weigl et al. The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility. Preprint. (2022) Proceedings of the Hawaii International Conference on System Sciences 2022. http://hdl.handle.net/10993/48537

[2] Johnson J (2014) From open data to information justice. *Ethics and Information Technology* 16(4): 263–274.

[3] Renieris E.M. Human Rights & the Pandemic: The Other Half of the Story. Carr Center Discussion Paper Series.

[4] Ishmaev et al. Ethics in the COVID-19 pandemic: myths, false dilemmas, and moral overload. Ethics and Information Technology (2021) https://doi.org/10.1007/s10676-020-09568-6

Department of Internal Affairs: Policy groundwork.

15. The policy papers repeat the scope arrived at in the early stages without addressing large problems and fleshing out pervasive challenges that are recognised internationally.

    a. *December 2016. Australian (sic) Post* – white paper not linked.[5]
    b. *June 2019*. Lobby Group Digital Identity NZ article: Nine out of 10 Kiwis want more control of their digital identity. (Link)
    c. *Combined Digital identity proactive release* (Link)
        i. 2 July 2020, Progressing Digital Identity: Establishing a Trust Framework Cabinet paper, (page 2)
        ii. Coversheet: Progressing Digital Identity: Establishing a Trust Framework (page 17)
        iii. 2 July 2020, Progressing Digital Identity: Establishing a Trust Framework Regulatory Impact Statement, Department of Internal Affairs (Impact Statement: A Digital Identity Trust Framework page 27)
        iv. 2 July 2020, Cabinet Government Administration and Expenditure Review Committee Minute of Decision, Digital Identity: Establishing a Trust Framework, Cabinet Office (page 55)
        v. 6 July 2020, Cabinet Minute of Decision, Report of the Cabinet Government Administration and Expenditure Review Committee: Period Ended 3 July 2020, Cabinet Office. (page 58)
    d. *14 May 2021: Proactive release of Cabinet material about Detailed Policy for a Digital Identity Trust Framework Bill* (Link). (Hon Dr David Clark, Minister for the Digital Economy and Communications.).
        i. 17 February 2021. Minute of Decision. Digital Identity Trust Framework Bill: Detailed Policy Proposals. Cabinet Economic Development Committee. (page 2)
        ii. 19 February 2021: Minute of Decision. Report of the Cabinet Economic Development Committee (page 8)
        iii. Appendix A Trust Framework Principles (page 30**)**
        iv. 10 February 2021. Regulatory Impact Statement: Detailed policy for a Digital Identity Trust Framework. (page 34-92 Link)
    e. 3 May 2021. Clark Speech on Digital Identity Trust Framework (Link)
    f. 11 August 2021. Regulatory Impact Statement: Additional policy decisions for the Digital Identity Services Trust Framework Bill. (Link)

16. The rationale for the DIB focusses on a governance and compliance regime:

    g. The Department of Internal Affairs identified that there was inconsistency and a lack of integration across the digital environment, and that as a result, there are inefficiencies, security and privacy risks and interoperability barriers. As a result, the DIA identified that a 'governance and compliance regime' was required to ensure that 'those who are providing digital identity services consistently meet legislation and standards for using, storing and sharing personal and organisational information'. (page 17/58)

[5] https://auspost.com.au/enterprise-gov/content/dam/corp/ent-gov/documents/digital-identity-white-paper.pdf

h. As a response the 'preferred government intervention' was established as *'implementation of a regulatory framework to ensure minimum standards are consistently applied across the digital identity ecosystem'*. This would involve:

   i. The establishment of a Digital Identity Trust Framework (Trust Framework) to set the rules (standards, legislation) for those participating in New Zealand's digital identity ecosystem.

   ii. The establishment of a governance board

   iii. The establishment of an accreditation team

   iv. The introduction of a new Bill to establish the powers of the Trust Framework, its governance board and accreditation team, as well as introduce amendments to pre-existing legislation to ensure alignment with the Trust Framework.

17. The faults, or narrow scope of the DIB are reflected in a rudimentary Purpose which appears to contain promises but does not build in an obligation that can speak to unanticipated challenges which potentially include human rights violations, and difficult to anticipate threats including technological development (such as AI) and data piracy. There is no evidence that the 'principles' and any consequent 'governance board' or 'accreditation team' would have sufficient insight that would assure appropriate oversight. This deficiency is reflected in the purposes of the future Act:

    3 Purpose
    The purposes of this Act are—
    (a) to establish a legal framework for the provision of secure and trusted digital identity services for individuals and organisations:
    (b) to establish governance and accreditation functions that are transparent and incorporate te ao Māori approaches to identity.

Consultation / stakeholder engagement

18. Considering the issues above, has appropriate stakeholder consultation been undertaken? The stakeholders were '*consulted on their views regarding the challenges with digital identity services and how they thought these could be addressed'*.[6]

19. The policy documents do not include formal analysis or white papers that have been published following the 'targeted consultation'.

20. It remains unclear how a digital framework was presented to stakeholders, and how the scope of consultation was handled. While the DIA appeared to identify 'four options' it is unclear if wider conversations concerning the governance of data, long-term risk and systems failure were addressed. A narrow set of problems appeared to be defined by the DIA and the stakeholders given the chance to respond.

21. Major documents following public consultation have not been supplied. Instead, simply brief summaries or 'key takeaways' which the public are asked to prima facie accept. The policy documents claim some 100 public, private and non-governmental entities have been consulted through 'face to face meetings, regular workshops, surveys and focus groups over an 18 month

[6] Impact Statement: A Digital Identity Trust Framework. Page 27.

period.' (33/58 Link) However no publication has been provided that provides detailed evidence of the scope and depth of the consultation.

22. Release of data/white papers are important as it can reveal the scope of consultation, the degree to which participants were able to enrichen discussion concerning digital identity systems, their benefits and risks, and the degree to which officials shaped consultation by giving participants choices to select from.

23. Text in 15 (c):

    a. Consultation (10/58) *The following agencies were consulted and are in general agreement with this paper: Accident Compensation Corporation, Department of the Prime Minister and Cabinet, Government Communications Security Bureau, Inland Revenue Department, Land Information New Zealand, Ministry of Business, Innovation and Employment, Ministry of Education, Ministry of Health, Ministry of Justice, Ministry of Primary Industries, Ministry of Social Development, New Zealand Customs Service, New Zealand Transport Agency, Office of Disability Issues, Office of the Privacy Commissioner, Social Wellbeing Agency, State Services Commission, Statistics New Zealand, Te Arawhiti, Te Puni Kōkiri and The Treasury*
    b. Officials engaged consistently with a working group that included a *wide variety of key public and private sector stakeholders. As well as public agencies, the working group included representatives from: ANZ, ASB, Auckland University, MATTR8, Payments NZ, Planit, Sphere Identity, SSS IT Security Experts, Two Black Labs, Westpac and Xero.*
    c. (25/58): *Option development was informed by extensive stakeholder engagement over the past 18 months. • This involved not only surveys and focus groups, but also consultation with over 100 organisations, including public agencies, Crown entities, digital service providers, financial institutions, academic institutions and a wide range of international partners*
    d. To ascertain the *views of these stakeholders, extensive consultation was undertaken both with individuals and over 100 public, private and non-governmental entities. This was achieved through face to face meetings, regular workshops, surveys and focus groups over an 18 month period. The key takeaways from this consultation are outlined below.*

24. Text in 15 (d) notes (page 12/92 link) that the *private digital service providers included MATTR, SSS online security consultants, Planit software testing, Middleware Solutions, SavvyKiwi, Sphere Identity and Xero. Financial institutions included Westpac, ASB, KiwiBank, ANZ, BNZ, Payments NZ and PartPay.* Otago and Auckland universities were consulted but the expertise of the actors included in the consultation remains unknown. Iwi groups appear restricted to the Iwi Chairs Forum and the Data Iwi Leaders Group – however 'future engagement' is promised.

25. Text in 15 (f) advises that ConsumerNZ were included in consultation. There is no indication any other public interest institute with a focus on human rights, ethics or any institution focussed on digital futures and the public interest were consulted.

26. The 15 (f) document advises that research and surveys were undertaken 2019-2020 but does not link to them (page 9/28). The policy was (page 11/28):

    'tested with targeted stakeholders between May and July 2021. Stakeholders consulted on the Bill's detailed policy proposals (including the options in this analysis on liability and pecuniary penalties) included:

    - *Representatives from the digital identity sector, including Digital Identity NZ members, MATTR, and independent consultants;*

- *Other organisations with an interest in the Trust Framework, including banks, Consumer NZ, Internet NZ and Payments NZ;*
- *Public service agencies and the Office of the Privacy Commissioner; and*
- *A Māori technical working group with subject matter expertise, including leaders from Māori digital identity initiatives and public service members with relevant Māori expertise.*

27. The public have been excluded from over two years of 'targeted engagement' or consultation. Targeted stakeholder consultation has excluded civil society organisations that might have an interest in the Trust Framework. [7] The February 2021 Regulatory Impact Statement: Detailed policy for a Digital Identity Trust Framework stated:

    'officials have undertaken targeted engagement with sector stakeholders and research bodies to gather a robust body of evidence, the Department has not publicly consulted on the detailed policy proposals considered in this paper' (5/59 Link).

28. There is no evidence of inclusion in the targeted consultation of public sector academic and research expertise that flesh out the inter-disciplinary legal, ethical and technical challenges across policy and legislation.

29. Which potential providers were involved in the consultation? We are aware that a consortium (ID2020) of powerful interests appear to be involved (see Appendix) [8]

30. It is not evident that other relevant actors, such as Catalyst, and the Linux Foundation, been included also. The public institutions that have been consulted with do not appear to have included public sector institutions and academics with a keen interest in the digital landscape. We cannot see the Catalyst Institute, Veracity Labs nor public interest groups such as the NZ Council for Civil Liberties included in the consultation.

31. The targeted consultation may have limited the potential for policy-makers and drafters of legislation to engage in higher level strategic issues concerning data integrity, data theft, corporate capture, single or multiple-use platforms and so on that would enable the development of a robust overarching values-based framework. This would inform both the quality and provenance of information used across the governance landscape, from policy development to regulatory judgements.

32. It is evident that the DIA are aware that the lack of public consultation throws a shadow over policy development:

    'To mitigate the risks around the lack of public consultation, the Department intends to seek Cabinet authority to release an exposure draft of the Bill. The release of the exposure draft will not seek feedback on whether the policy proposals considered in this RIS should be reviewed or changed. Rather, it will provide the public with the opportunity to comment on whether the Bill gives appropriate effect to these policy proposals (e.g. whether the Authority's enforcement powers regime achieves the objective of ensuring compliance with the Trust Framework). (5/59)

33. The only so-called public feedback, comes from the *Digital Identity* lobby group.

---

[7] Regulatory Impact Statement: Additional policy decisions for the Digital Identity Services Trust Framework Bill. P.11 https://www.dia.govt.nz/diawebsite.nsf/Files/detailed-policy-for-the-digital-identity-trust-framework/$file/RIS-Additional-policy-decisions-for-the-Digital-Identity-Services-Trust-Framework.pdf

[8] COVID Credentials Initiative ("CCI") i https://www.covidcreds.org/

a. Clark's May 3 speech noted, concerning trust that 'Research conducted with New Zealanders in 2020 highlights that a majority of participants trusted local websites with their identity information more than other websites'. This research appears to have come from a lobby group which represents powerful industry interests (see Appendix) rather than a public interest organisation.

34. The DIB and supporting policy makes oblique references to 'risks' and 'gaps' but these risks and gaps are not extended to an analysis of what the risks might be, and which potentially might include surveillance, commodification of data and undisclosed conflicts of interest across Trust Framework providers between advisers to the governance board or the accreditation team.

35. The increased exchange of sensitive data requires digital cooperation through interconnected databases. 'This results in a paradox where electronic identification systems enhance security on the one hand, but may compromise users' privacy on the other. Eventually, data collection, cross-referencing, and the aggregation of metadata could lead to surveillance by the state or third parties'.

36. The policy appears to underestimate or sideline the profound governance and stewardship challenges of establishing robust and trustworthy digital identity. Europe has a far more advanced policy platform, yet their scientists urge that less emphasis is placed on 'efficiency' and more time is taken to address underlying complexities. [9] By advocating for greater foresight, there is less risk that bad design choices will be made that 'squander trust'. The scientists emphasised that digital identity platforms are ambitious projects that should be 'done right', noting that timelines 'should be driven by technological readiness rather than political considerations'. They also stated that:

Social justice considerations should be given equal priority, so the European Digital Identity does not become yet another 'login with X' button. [10]

37. Without adequate consultation to deepen the policy, we consider that potential for a status quo to be arrived at that does not place the public interest at the centre of policy. As Duncan and Chapple have discussed[11], and has been borne out in our past experiences in submitting to proposed legislation, we know from past experience that once a 'regime' or framework is installed it is very difficult to shift, and we predict that the powerful interests that will benefit from the current weak form of policy will work to lock the current framework in, which creates additional barriers to public participation and/or contestation.

Ignoring the direct and indirect influence of Big Data

38. New Zealand's governing institutions pale in comparison with the interconnected networks of powerful interests that increasingly consolidate as oligopolies as 'big data'.

39. Market failures arise when there are information asymmetries, and when there are non-competitive markets (such as the potential for offshore owned 'big data' to exert a disproportionate influence).

40. Potential for large service providers (as vested interests) to exert asymmetrical market-power (enjoy an unfair advantage) based on resources and knowledge. The power (and knowledge) imbalance can

[9] Rieger et al. Letter to the editor. Not yet another digital identity. *Nature Human Behaviour*. November 2021 doi 10.1038/s41562-021-01243-0
[10] Ibid
[11] Duncan G. & Chapple S. What is a vested interest? *Policy Quarterly* May 2021. 17:2:3-8

result in a tendency for governing bodies to 'turn a blind eye to' conflicts of interest and data exploitation.

41. This policy that informs this DIB is produced in an institutional environment surrounded by increasingly concentrated power:

    'Since 2001, five leading technology companies have avoided antitrust enforcement to complete over 600 mergers. Through uncontested acquisitions they have dominated markets, eliminated rivals and grown so powerful that their influence over human affairs equals that of many governments. Accordingly, lawmakers, scholars and antitrust regulators increasingly call for restraints on their power.'[12]

    Marks has identified this phenomenon as 'biopower', which arises (1) through unprecedented concentrated private influence; which can (2) be transformed into other forms of influence including market power and political power (as coercive influence); and which may (3) harm competition, erect barriers to entry, displace small firms and threaten social, political and economic liberty.[13] Marks has warned that:

    'companies can leverage cross-market data flows to exert biopower in numerous markets, providing unprecedented influence over many spheres of human activity. Some antitrust scholars and regulators seem to comprehend the significance of this power. However, they lack the vocabulary adequately characterize it and the theoretical power to operationalise it'[14]

42. McKinsey has acknowledged: *'Administrators of a digital ID system could misuse digital ID for economic or noneconomic reasons—for example, to profit from the collection and storage of personal data or for surveillance, targeting, and persecution of individuals or groups.'*[15]

43. Highlighting the potential for powerful interests is not only important to recognise risk to the individual, it an important for upholding technological sovereignty – where the sovereign is:

    'not the isolated individual, but the city as a collective, that is the community of citizens who should be able to exercise "full control and autonomy of their Information and Communications Technologies (ICTs), including service infrastructures, websites, applications and data, in compliance with and with the support of laws that protect the interests of municipalities and their citizens'[16]

44. This can only be upheld through transparent, consultative democratic platforms that are effectively resourced.

45. Officials remain silent on these issues. Without these issues addressed in overarching policy, a policy vacuum occurs, where the norms and values are established by powerful institutional interests. [17] The

---

[12] Marks M., Biosupremacy: Big Data, Antitrust, and Monopolistic Power Over Human Behavior (September 19, 2020). 55 *U.C. Davis Law Review 101* (2021, forthcoming), Available at SSRN: https://ssrn.com/abstract=3695373 page 104

[13] Ibid. p.105

[14] Ibid p.110

[15] McKinsey. (2019) Digital identification: A key to inclusive growth. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20identification%20a%20key%20to%20inclusive%20growth/mgi-digital-identification-report.pdf

[16] De Rosnay D. & Stalder F. Digital Commons. *Internet Policy Review*, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 9, Iss. 4, pp. 1-22, http://dx.doi.org/10.14763/2020.4.1530

[17] Andersson J. The Quiet Agglomeration of Data: How Piracy is Made Mundane. *International Journal of Communication* 6 (2012), 585–605

consequence, as a recent article on Singapore explained is that 'technology gets built to solve problems for the government, rather than for citizens.'[18]

Market-friendly scope of consultation

46. Evaluation of risks has been inadequate. The 'Progressing Digital Identity: Establishing a Trust Framework' proposal identified risks or gaps that appear identified as problematic – however the policy documents focus on gaps that obstruct innovation rather than risks to the public interest.

47. The OECD define innovation as '"the implementation of a new or significantly improved product (good or service) or process, a new marketing method, or a new organisational method in business practices, workplace organisation or external relations".[19]

48. The gaps identified in the paper identified (5/58):

    a. The problem of limited control by people how information is used, and peoples concerns that they would be unnecessarily exposed to privacy and security risks

    b. Lack of efficiency and coordination between the public-private sector 'making user-consented information sharing more difficult and resulting in services that cannot work with each other in a trusted way'.

    c. A lack of governance and structure resulting in inconsistent laws and standards making user-consented information sharing difficult, and uneven application in the private and public sectors.

49. The paper also noted 'inconsistent application of data privacy, identification and security standards can lead to systematic issues and breaches. This poses risks to both customers and businesses, undermining trust and confidence in the digital identity ecosystem further and slowing adoption.'

Efficiency at what cost.

50. The focus of governments on 'efficiency' (as is evident across the policy documents) can result in the undermining of important ethics and values-based issues central to the public interest.

51. A focus on technical efficiency, considering only instrumental solutions – and deterring more complex consultation in the short term effectively works to weaken the production of more robust parameters which are protective over the longer term.

52. A rhetoric of efficiency obscures the fact that 'efficiency' is rarely understood. While associated with economic rationalism, 'the doctrine that economies, markets and money can always, at least in principle, deliver better outcomes than states bureaucracies and the law' – economic rationalism fails to take account of intertemporal, complex socio-political realities. Patrick O'Keefe has argued that 'efficiency' is often pursued 'in spite of' rather than for the betterment of society.

53. We do not consider that the current policy platform is sufficiently transparent, accountable and enforceable, and because of this, greater cross-government and public debate is required.

---

[18] Guest P. Singapore's tech-utopia dream is turning into a surveillance state nightmare. Nov 16, 2021. https://restofworld.org/2021/singapores-tech-utopia-dream-is-turning-into-a-surveillance-state-nightmare/?utm-source=sharing

[19] OECD. (2005). The Measurement of Scientific and Technological Activities, Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data, 3rd edition,. A joint publication of OECD and Eurostat.

54. There is evidence of activity. Principles have been arrived at; apparent consultation with some stakeholders has occurred; stakeholders have been given some options to comment upon. However, there is no evidence of deep inquiry that can address uncertain complex socio-political and socio-technical issues by policy-makers.

Human Rights.

55. Policy Papers (listed in section 17 above) claim there are no human rights impacts:

    a. Text in 17 (c) states here are no human rights implications from this paper (page 13).

    b. Text in 17 (d) states *'there are no immediate impacts on human rights arising from the proposal outlined in this paper as all information sharing requires user consent'* going on to state:

    '*it is important that the proposal is implemented in alignment with ongoing work to improve digital inclusion across government and to support Article 21 of the Universal Declaration of Human Rights (everyone has the right of equal access to public service in their country). This means ensuring accessibility for disabled people, refugees and migrants, and that indigenous rights, data sovereignty and the principles of the te Tiriti o Waitangi are consistently upheld. The design of the proposed Trust Framework and surrounding ecosystem will also allow for alternative channels for proofing identity to be available to those who cannot or choose not to participate*' (pages 22-23). Later in the principles, it is stated that '*the rights and needs of people are paramount, though not to the exclusion of the needs of other entities in the digital identity ecosystem'* (page 25).

56. However there is no policy that articulates how rights will be ensured. All too often, economic, social, and cultural rights remain outside these discussions.[20]

57. Privacy as a human right is too often misleadingly represented as simply an individual value.[21]

58. There is no discussion on the relationship between self-determination and individual autonomy and how this might be protected.[22] [23]

59. States formal commitments to human rights protections are often decoupled from actual practices.[24] The absence of a values-based framework iterating potential human rights implications, removes a policy framework that can prevent this risk of decoupling of general values from practical action. Without deliberation with human rights experts, claims that there are no human right implications lack foundation.

---

[20] Renieris E.M. Human Rights & the Pandemic: The Other Half of the Story. Carr Center Discussion Paper Series.

[21] Ishmaev et al. Ethics in the COVID-19 pandemic: myths, false dilemmas, and moral overload. Ethics and Information Technology (2021) https://doi.org/10.1007/s10676-020-09568-6

[22] 'Self-determination under Article 1 of the ICCPR invokes protection of the "private sphere" as advocated by Charles Reich. "the individual sector" according to Reich is the "zone of individual power' necessary for the healthy development and functioning of the individual" and "absolutely essential to the health and survival of democratic society" A right to identity is part of that personal sphere, and arguably it now includes the right to digital identity. Digital identity is protected under Article 1(1) of the ICCPR because the Article protects individual autonomy and is directly relevant to digital identity because it purports to give the individual control over his/her identity information and who can access it.'

[23] Sullivan C. Digital identity – From emergent legal concept to new reality. *Computer Law & Security Review* (2018) 38:723-731. Page 731.

[24] Goodman R. & Jinks D. Incomplete Internalization and Compliance with Human Rights Law. *The European Journal of International Law* (2008) 19:4

60. Developments in artificial intelligence may outpace and obstruct rights protections.

    a. A European White Paper stated: "the specific characteristics of many AI technologies, including opacity ('black box-effect'), complexity, unpredictability and partially autonomous behaviour, may make it hard to verify compliance with, and may hamper the effective enforcement of, rules of existing EU law meant to protect fundamental rights"[25]

    b. Substantial barriers exist for researchers to parse apart and understand the relationship of artificial intelligence and surveillance and the potential for this to encroach on civil and bodily liberties, particularly for traditionally marginalised groups.[26]

61. The technical approach has recognised the power of data to be applied to identity, but has not connected this to a social justice framework, or agenda. As Linnet Taylor has discussed, 'although data-driven discrimination is advancing at a similar pace to data processing technologies, awareness and mechanisms for combating it are not [27]

    a. The Trust Privacy Principles focus on 'Māori approaches to identity' and ignore the potential for data identity systems to perpetuate inequalities. Simply assuring privacy through the Privacy Act is not sufficient to protect vulnerable communities.

    b. Digital identity systems have power to generate forms of structural discrimination (embedded in institutions, rules, and practices), and multiply social disadvantage. [28]

62. The public cannot assume the 'opt out' framework will not exert soft power.

    e. While the policy documents claim that the digital identity is voluntary and that citizens can opt out, it is very clear from international developments (such as in India and China) that participation in digital identity systems will increasingly become a requirement in order to receive welfare benefits, sign up for mobile phones, confirm identity for voting and register at school.

    f. The legislation could change. Such changes have potential to producing a ratcheting effect, further decoupling oversight regimes from human rights obligations without appropriate input from the public.

    g. The passing of a huge body of legislation during the Sars-Cov-2 pandemic revealed that the government can and will swiftly enact legislation without appropriate consultation. In addition, when consultation has been undertaken, the state's decision may not reflect the perspective, or weight of public comment.

    h. Opt-out may be possible but result in lack of access to previously accessible welfare state benefits. For example, it may be difficult to formally register for, or access benefits or services.

    i. For example, the European General Data Protection Regulation 2016/679 (GDPR) – such as consent may be withdrawn as freely as it is given.

---

[25] White Paper On Artificial Intelligence—A European approach to excellence and trust. European Commission, Brussels, 19.2.2020 COM(2020) 65 fnal, p. 12.
[26] Smith GJD. The politics of algorithmic governance in the black box city. *Big Data & Society*. (2020) doi 10.1177/2053951720933989
[27] Taylor L. What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*. 2017:1-14. Doi 10.1177/2053951717736335
[28] Ibid

Unresolved issues: The Bill raises as many questions relating to trust

63. It is not evident that an overarching 'Trust Framework' has been established in such a way as to address and anticipate the challenges identified in the Cabinet problem identification paper.

64. Failure to monitor and assess the global environment: There is no evidence of a review of global best practice and nor a review of the state of global development of digital identity regulatory environments. The potential to interlink with global research forums which specifically focus on public-good digital identity development including open-source software appears not to have been undertaken.

65. The governance group should clearly identify a requirement for advisors from public interest public sector institutions that can provide intelligence that may counter the claims of private industry. There is no clarity on who informs the representatives from the Government Chief Digital Officer the 'GCDO, the Government Chief Information Security Officer, the Government Chief Data Steward, the Office of the Privacy Commissioner and Māori.'

66. There is no discussion or analysis on the architecture of the digital identity framework, for example the benefits and risks of centralised/decentralised platforms. For example:

    'particularly libertarian societies gravitate towards decentralized technologies that 'liberate' citizens from centralization and control. However, the decentralization of digital identity management systems also starts to attract the interest of societies that place a higher trust in institutions.'[29]

67. Failure to build in intelligence mechanisms (an adequate expert research quorum) that enable New Zealand to respond to both the dynamic nature of the digital environment and new knowledge internationally.

    a. For example, big data technology has uneven effects on small and large firms. Institutional shifts result in aggregation of power towards cartel-like or monopoly environments.[30] [31]

68. The softness of the penalties (as enforcement) infers 'light touch' regulation. There is a conflict between a financial penalty that will be effective for a smaller local provider, that will simply be viewed as a 'light touch tax' for a larger, offshore owned institution. We consider that the pecuniary penalties insufficiently take account of the potential for large service providers to view penalties as they stand as merely the cost of doing business.

    a. There is no discussion on the risk where TF providers have direct conflicts of interest, such as institutional interests with the technological and commercial capability to exploit private data.

    b. The financial penalties are narrowly defined and do not transparently include penalties for example, following transfer of information to a third party.

    c. How might penalties be obstructed by international trade agreements?

---

[29] Weigl et al. The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility. Preprint. (2022) Proceedings of the Hawaii International Conference on System Sciences 2022. http://hdl.handle.net/10993/48537

[30] See Monopolization Defined, FED. TRADE COMM'N, https://www.ftc.gov/tipsadvice/competition-guidance/guide-antitrust-laws/single firmconduct/monopolization-defined (last visited Dec. 29, 2020) [https://perma.cc/TYL5-U488] (defining a monopolist as a firm with significant and durable market power characterized by the long-term ability to raise prices or exclude competitors).

[31] Marks M., Biosupremacy: Big Data, Antitrust, and Monopolistic Power Over Human Behavior (September 19, 2020). 55 *U.C. Davis Law Review* 101 (2021, forthcoming), Available at SSRN: https://ssrn.com/abstract=3695373

69. Consolidation of power in large private institutions is discussed below. The intertemporal nature of data management- long term stewardship of data exposes the New Zealand public and the Crown to distinct economic vulnerabilities. Over time as private sector Trust Framework providers aggregate power and knowledge, they will be able to exert greater financial pressure on the Crown as rentiers, and demand higher rates for their services. It is anticipated that they will increasingly seek to monetise that data (as rentiers).

70. Liability – reliance on a complaints mechanism is inadequate for the job.

    a. A complaints mechanism is inadequate (not proportionate) to the risk, relying on post-facto complaints, and the potential for citizens or public sector actors to have adequate resources

    b. Governing bodies should be obligated to annually submit a report and analysis of international court decisions relating to digital identity across a wide range of economic, social, cultural and human rights based issues.

    c. The policy and DIB assume that citizens will be prompted by acute events to undertake proceedings. However, activities that result in rights interventions can be much more mundane and difficult to identify. Data piracy and digital reproduction is more nebulous, as the 'commons' can be held by the private sector, and lacking appropriate stewardship , they are:

    'governed not by state and federal laws and regulations, but by systems of more and less explicit norms developed by the practitioners themselves. Historically such commons have been small-scale, but online they become translocal, potentially global in reach and scale'.[32]

    d. The August 2021 Regulatory Impact Statement (RIA)[33] accepts that 'there is a lack of clarity as to when and how liability for loss would apply in civil claims to actors operating or using digital identity services. It is therefore unclear whether liability would properly be applied to those whose actions are responsible for harm and when accredited digital identity service providers would be protected from liability for harm resulting from reliance on their services.'

    e. There seems to be excessive reliance on the new Privacy Act. From our understanding, the Privacy Act aims to assert an 'individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognising that other rights and interests may at times also need to be taken into account'. The Privacy Act may not prevent organisations from securing data.

71. There is a lack of policy or legal clarity relating to the New Zealand governments responsibility to protect the public interest where service providers use artificial intelligence and apply algorithm based decision-making and prediction models.[34]

---

[32] Andersson J. The Quiet Agglomeration of Data: How Piracy is Made Mundane. *International Journal of Communication* 6 (2012), 585–605

[33] Regulatory Impact Statement: Additional policy decisions for the Digital Identity Services Trust Framework Bill https://www.dia.govt.nz/diawebsite.nsf/Files/detailed-policy-for-the-digital-identity-trust-framework/$file/RIS-Additional-policy-decisions-for-the-Digital-Identity-Services-Trust-Framework.pdf

[34] Kerikmäe T. & Pärn-Lee E. Legal dilemmas of Estonian artificial intelligence strategy: in between of e-society and global race. *AI & Society* (2021) 36:561–572 https://doi.org/10.1007/s00146-020-01009-8

a. For example, the policy appears to inadequately recognise the implications of regulating *knowledge* technology (as opposed to regulating information technology).

b. Current data protection law cannot meaningfully regulate machine learning algorithms.[35]

c. AI deserves a critical stance in order to apply judgement. AI technologies may not necessarily result in benefit, and they may also result in a 'moral fog' produced by the creation of risks that undermine the integrity of public services. [36]

d. Similarly, lacking an overarching values framework, the policy is unable to direct future automation that might be protective of the public interest.[37]

How will trade agreements impact local sovereignty and decision-making?

72. Trade agreements have been found to exert a chilling effect on democratic governance. For example, simply the threat of litigation may stall actions to protect the public interest.[38] [39] [40]

73. Where is the analysis regarding the potential for the Digital Economic Partnership Agreement (DEPA) to impact decision-making with regards to this DIB.

74. Will trade agreements such as the Regional Comprehensive Economic Partnership (RCEP) and Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP) impact selection of providers and the potential to take regulatory action? result in the privileging of offshore institutions for contracts over domestic public or private providers?

    a. How do the e-commerce provisions impact decision-making, such as control over data, where data is located, who controls access to source codes and algorithms, and whether the provider is even located in New Zealand?

    b. Is it much easier to break a contract with a local provider than an international TF provider?

    c. Do agreement provisions reduce the potential for government regulators to respond proportionately to deter risk of system error, confidentiality breaches or fraud-based activities by organisation size and market power?

75. How does the DIB intersect with trade agreements and te Tiriti o Waitangi/the Treaty of Waitangi? A recent report by the Waitangi Tribunal found the electronic commerce (e-commerce) provisions in the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP) breached the Crown's Tiriti/Treaty obligations to actively protect Māori rights and interests. The report made the following observations:

---

[35] Gellert R. Comparing definitions of data and information in data protection law and machine learning: A useful way forward to meaningfully regulate algorithms? *Regulation & Governance* (2020) doi:10.1111/rego.12349

[36] Ishmaev et al. Ethics in the COVID-19 pandemic: myths, false dilemmas, and moral overload. Ethics and Information Technology (2021) https://doi.org/10.1007/s10676-020-09568-6

[37] Tsalakalis et al. The dual function of explanations: Why it is useful to compute explanations. *Computer Law & Security Review*. 41:105527

[38] Cooper et al. Seeking a Regulatory Chill in Canada: The Dow Agrosciences NAFTA Chapter 11 Challenge to the Quebec Pesticides Management Code, 7 Golden Gate U. *Envtl. L.J.* 5 (2014).

[39] Cote, C. (2018) A chilling effect? Are international investment agreements hindering government's regulatory autonomy? International Trade Law and Regulation, 24 (2). 51 - 61. ISSN 1357-3136

[40] Moehlecke C. The Chilling Effect of International Investment Disputes: Limited Challenges to State Sovereignty. *International Studies Quarterly.* 64:1:1-12

a. ‘we recognise that from a te ao Māori perspective the way the digital domain is governed and regulated has important implications for the integrity of the Māori knowledge system, which is unquestionably a taonga. The vulnerability of taonga such as mātauranga Māori mean that the Crown’s Tiriti / Treaty duty of active protection is heightened.’ [41]

76. The Waitangi Tribunal Report concluded:

a. ‘we do not share the Crown’s confidence that Māori rights and interests in the digital domain are unaffected by the e-commerce provisions in the CPTPP’

b. ‘the policy space retained by the CPTPP exceptions and exclusions is not as extensive as the Crown maintains. We also conclude there is a material risk of regulatory chill and risk arising from the precedent or ratchet effect of the CPTPP e-commerce provisions.’

c. ‘the risks to Māori interests arising from the e-commerce provisions of the CPTPP are significant, and that reliance on the exceptions and exclusions to mitigate that risk falls short of the Crown’s duty of active protection.’

d. the Crown has failed to meet te Tiriti / the Treaty standard of active protection. We conclude that this failure constitutes a breach of te Tiriti / the Treaty principles of partnership and active protection[42]

77. Non-accredited digital identity service providers are not required to comply with the rules. This point alone should be sufficient to prompt a ‘go slow’ on the DIB.

78. *Electronic identification* There is only mention of a natural person. eIDAS definition ‘electronic identification’ means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person. Is this important?

79. Commercially sensitive information: Section 61 states that ‘authority must not release any information or document received by it under this section if the information or document is commercially sensitive’. This generic statement carries the capacity to stifle Official Information Act requests as there are no boundaries around what ‘commercially sensitive’ information may constitute. Should this be more deeply debated?

80. The digital environment is highly dynamic, and we consider greater deliberation is required in order to provide an overarching structure that can robustly navigate the complexity, uncertainty and ambiguity inherent in digital identity services.

Articulation of Risk

81. Governance of digital identity must also encompass the governance of public-good technological, legal, ethics-based and technical institutions that effectively act as intelligence to inform investment to predict and navigate threats and counter the claims of the private sector.

---

[41] Ministry of Justice. The Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership. Pre-publication version. WAI 2522. Waitangi Tribunal Report 2021. *Waitangi Tribunal,* Wellington, New Zealand. Page xii

[42] Ministry of Justice. The Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership. Pre-publication version. WAI 2522. Waitangi Tribunal Report 2021. *Waitangi Tribunal,* Wellington, New Zealand. Pages xiii-xiv

a. As an example, scholars have cited the fast-moving pace of artificial intelligence and the internet of things and emphasised that higher level political and economic strategies should be in place before legal standards are enacted.[43]

82. Risks are envisaged to concern non-compliance of providers – however what exactly constitutes a degree and potential of non-compliance, remains unaddressed. Risk to digital service providers arising from legal liability is discussed. The Bill provides (Part 7) that the Trust Framework providers are immune from civil liability unless they 'act in a manner, relating to the alleged harm or damage, that constitutes bad faith or gross negligence.'

    a. It is unclear whether there are other channels that enable citizens to protect their right to identity. Legal liability may act as a barrier to action to protect this right.[44]

83. Mechanisms to identify failure are inadequate and disproportionate to public risk. Currently, 'Bill allows for people to submit complaints to the TF authority if they believe a TF provider has breached 1 or more of the TF rules, the regulations, terms of use of trust marks, or the Act'.[45] In such an environment where the balance of power is in favour of large industry interests, the regulator must adopt a proactive rather than reactive position. Therefore, any legislation requires the establishment of an independent Commissioner with a mandate and funding to conduct active, ongoing independent investigatory work. This work should not be limited to New Zealand, but to the activities of TF providers in foreign jurisdictions, including evidence of malfeasance, court action and participation in foreign deliberation concerning digital identity services.

84. Recognition of risk is based on investment in science & technology that may turn up 'uncomfortable knowledge'.

    a. The conditions for production of science and technological knowledge that can inform government policy is heavily dependent on the policy conditions, as governance, that enable the production of that knowledge.

    b. Where knowledge potentially undermines the principles of powerful interests, or may produce a deleterious effect on the goals of powerful interests – that knowledge is considered uncomfortable knowledge. Institutions can then work to deny, dismiss, displace, or divert resources away from that knowledge.[46]

85. Complexity, uncertainty and ambiguity is a central feature of risk governance.[47] There are many intervening factors affecting the relationship between the management of data and the capacity for that data to be private and secure through numerous providers in the service chain (the environment is complex). There is substantial uncertainty: how is data curated across different providers; data ownership remains uncertain, as does the potential for the state to provide adequate protections for the public when data is managed by offshore institutions. There is substantial ambiguity, the legislation asserts that stewardship will be compatible with the Privacy Act, but then appears to base recognition of market-failure around a complaints mechanism. In addition, there is no discussion on the potential for trust framework service providers to exploit and incorporate data for use in other

---

[43] Kerikmäe T. & Pärn-Lee E. Legal dilemmas of Estonian artificial intelligence strategy: in between of e-society and global race. *AI & Society* (2021) 36:561–572 https://doi.org/10.1007/s00146-020-01009-8

[44] Sullivan C. Digital identity – From emergent legal concept to new reality. *Computer Law & Security Review* (2018) 38:723-731

[45] Digital Identity Services Trust Framework Bill Government Bill. Explanatory note.

[46] Rayner, S. (2012). Uncomfortable knowledge: the social construction of ignorance in science and environmental policy discourses. Economy and Society, 41(1), 107-125.

[47] Renn, O. Stakeholder and Public Involvement in Risk Governance. *Int J Disaster Risk Sci* (2015) 6:8–20. DOI 10.1007/s13753-015-0037-6

applications, and no discussion on the ownership of the data (and the potential for private gain). The value of this data is relatively difficult for the public actor to estimate but will be much more greatly understood by private institutions.

86. As Renn has discussed, these features - complexity, uncertainty and ambiguity- require that stakeholder engagement is more broadly engaged in order to strengthen policy responses. Technical and legal expertise are central pillars required to produce good legislation, but so is robust 'uncomfortable' that can flesh out the uncertainties, identify central values and more accurately characterise uncertainties.

Governance Anglo Style

87. While focus in Cabinet is on integration with Anglo nations, there is no evidence that work has been undertaken to identify the importance of human rights and anticipatory protections that might reflect European Union and European digital single market regulatory oversight through the General Data Protection Regulation.

88. Public sector ignorance is produced through the simple underfunding of institutions and areas of expertise that traditionally questioned power – that produce uncomfortable knowledge.

89. As Renn has discussed, these features - complexity, uncertainty and ambiguity- require that stakeholder engagement is more broadly engaged in order to strengthen policy responses. Technical and legal expertise are central pillars required to produce good legislation, but so is robust 'uncomfortable' that can flesh out the uncertainties, identify central values and more accurately characterise uncertainties.

90. Science and technology – and innovation – is central to the development of resilience, public wellbeing and economic growth. Yet New Zealand and sibling Anglo nations have been deeply compromised following 30 years of neoliberal governance which have not provided a research platform for scientific enquiry and scrutiny that can critique and challenge commercial science and technology claims. Scientists and researchers seeking to undertake such work find it extraordinarily difficult to secure safe, long-term funding.

91. The 3-decade pivot to the market, and the valorising of market-economics has reduced a place for critical practice and the public interest. In practice, the effect throughout universities and research institutions, has been a muffling of critical thought. Critical thought is necessarily uncomfortable, however it provides the space for deliberation and debate that can sow the seeds – and nurture - innovation and radical change that can challenge vested interests, but also monopolies who (implicitly and explicitly) secure power, and whose actions reduce the place for agile, integrated and democratically accountable innovation.

92. As we observe in the policy documents, New Zealand follows and turns narrowly to the other Anglo nations for both information and to provide regulatory legitimacy in order to secure social licence when legislation to govern new technologies are developed. This narrowed focus on the other colonial nations prevents us looking to older and perhaps more democratically accountable nations who might provide guidance and foresight when developing robust legislation and regulation.

93. New Zealand has different obligations, imposed through the Treaty of Waitangi.

Time to assess the costs and benefits of 'efficient' 'Contracting Out' cultures

94. If democracy is to be protected – strategic insight must reside inside the public sector.

    a. Reliance on third parties risk undermining the public interest, particularly if regulatory oversight is weak. Third party (as contractors or subcontractors) suppliers lack a civil service culture and that do not carry long-term knowledge into the public sector and that may evade transparent and accountable norms required for public servants.

    b. Mariana Mazzucato has advised European governments[48] on how reliance on the contracting out of projects reduces the capacity for governments to understand problems and anticipate problems. Without experience of the underlying science and technology, it is impossible to effectively manage ongoing contracts. This produces barriers to long-term (anticipatory) stewardship as governments lack the practical and applied knowledge and insight to appropriately govern these complex areas.

    c. Mazzucato discussed the importance of 'retaining 'absorptive capacity' 'i.e. the need to invest internally in knowledge creation so as to understand and interact dynamically with external opportunities [and threats] when they arise'.[49]

    d. Mazzucato's policy work helps provide an impetus to public investment in important missions and the importance of investment in public assets, especially that relate to protection of human and environmental health. These missions require long-term strategic thinking; are evolving and dynamic; and involve protection of the public interest.

    e. Extensive reliance on third parties, produce ignorance in the public sector, particularly with regards to the stewardship of science and technology.

95. Neoliberal governments have been reluctant to fund public good science and research with a mandate to explore new technologies and science in order to evaluate their short- and long-term impact on human and environmental health.[50]

    a. Regulatory capture is a natural consequence of the under-funding of regulatory institutions and the underfunding of a scientific/technological fora that provides feedback loops into the regulatory environment.[51] The regulators default to industry 'wisdom' and become technical experts but lack awareness of overarching situation complexity and are unable to anticipate threats. As an example of a failure to provide a stable scientific community that can inform and challenge the regulatory sphere, we cite the sustained and profound underfunding of environmental science research in New Zealand, the failure of the state to effectively articulate pollution in the new resource management policy.[52]

    b. Governance of science and technology directly impacts research content. For 3 decades, the science knowledge system has been transformed as funding has shifted to short term project-based support; as government agendas have been linked to funding schemes; as management

---

[48] Mazzucato M 2018a Missions: Mission-Oriented Research & Innovation in the European Union. European Commission. https://ec.europa.eu/info/sites/info/files/mazzucato_report_2018.pdf

[49] Mazzucato M. Mission Economy. A Moonshot Guide to Changing Capitalism. Allen Lane 2021

[50] Gross M. & McGoey (Eds.), Routledge International Handbook of Ignorance Studies (pp. 141-154). *Routledge.*

[51] PSGR see e.g. Submission to the Environment Select Committee 2021 Hazardous Substances and New Organisms (Hazardous Substances Assessments) Amendment Bill October 2021. https://psgr.org.nz/pub-res/submissions/nzepa/247-trusted-regulator

[52] PSGR Submission to the Environment Select Committee, 2021 Inquiry on the Natural and Built Environments Bill: Parliamentary Paper. August 2021. https://psgr.org.nz/pub-res/submissions/rma/234-2021rma

has become increasingly administration focused and as private-public partnerships have played a greater role in research development.[53]

c. Science and technology research policy currently shapes research towards innovation that results in a good or service (as I.P. for example) and towards securing finance from the private sector in order to promote economic growth. In heavily contested funding environments, public good research that lacks the 'teeth' of a more ambiguous 'public good' proposal will be scored lower in funding rounds.

d. The 'public interest' information environment that should inform this has been severely eroded over the previous 3 decades of new public management strategies which emphasise cost accountability, contract management and efficiency.[54]

e. Over this same period, there has been an exponential rise in big data and artificial intelligence, as the fourth industrial revolution.[55] However investment in public interest research to steward such information has not proportionately increased. This leaves democratic nations overly reliant on industry supplied data.

96. Of particular concern is the rise of the technology that underpins surveillance capitalism, which Zuboff emphasises:

> 'is not the same as algorithms or sensors, machine intelligence or platforms, though it depends on all of these to express its will. If technology is bone and muscle, surveillance capitalism is the soft tissue that binds the elements and directs them into action. Surveillance capitalism is an economic creation, and it is therefore subject to democratic contest, debate, revision, constraint, oversight, and may even be outlawed.'[56]

Conclusion: Trust Framework Principles cannot be upheld

97. The Digital Identity Services Trust Framework Bill (DIB) is premature and broader consultation is required.

98. While digital-identity platforms are required, this proposed DIB is inadequate: in particular, it does not address an accumulation of serious digital-identity abuse problems; it seems to make too much of an assumption that the issues are within the New Zealand jurisdiction when the global nature of data makes a nonsense of such a notion; its formulation lacks any due consideration of international public law and inter-jurisdictional cooperation; the DIB lacks a clear purpose and a clear intent to protect New Zealand people and New Zealand interests from exploitation and vulnerabilities; and it lacks flexible functions and powers that can address, in a timely fashion, emerging new threats to New Zealand people and New Zealand interests.

99. The policy-formulation framework does not produce a space for harvesting expertise that lies in the private sector that is involved with development of *new* digital platforms so that initiatives can be 'shaped' pro-actively to avoid damage to New Zealand people and New Zealand security interests.

---

[53] Gläser, J., & Laudel, G. (2016). Governing Science how science policy shapes research content. *European Journal of Sociology*, 57(1), 117-168.

[54] Gruening, G. (2001). Origin and theoretical basis of New Public Management. *International Public Management Journal*, 4, 1-25.

[55] Soni et al (2018) Impact of Artificial Intelligence on Business," in Digital Innovations, Transformation, and Society Conference 2018 (Digits 2018). 2018:10

[56] Zuboff S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*. 2019:1;10-29

100. In a similar context, New Zealand has made no commitment to developing a solid base of public good science and technology institutions free of conflicts of interest that can play an essential role in preparing, in advance, effective controls for emerging digital-technology risks; there is little point in positioning New Zealand in a 'reactive' mode to such risks because trying to recover what has been lost is too difficult; prevention is easier and cheaper than rectification. A 'comprehensive engineering' approach is needed. [57]

101. The Trust Framework Principles (Appendix A page 30/92) amount to promises or assurances, however they are insufficiently fleshed out in the supporting policy literature. The digital environment is highly opaque: an individual has little power to address conflicts or exploitation of data. It is the integration of digital data over time that is of the essence: the Bill does not seem to address that reality. Out-of-jurisdiction initiatives to cull data out of New Zealand people and businesses are another factor requiring more robust statutory provisions.

102. Data and information are the currency of the 21st century. The data of individuals has direct commercial value. There is potential for public sector actors to apply the information for the benefit of the state, such as to modify behaviour or for other coercive purposes, eroding the obligations of the state to protect the public interest.

103. This topic is a matter that has most important national security implications: we now live in a world of liminal warfare where the digital realm is a new playground for predatory states and powerful institutions to push their agendas-of-influence and control.

104. Such problems have not been identified in the policy documents. Without identifying these factors, there is potential to engage providers that have conflicts of interest, and who may be in a position to exploit this data for private gain. [This is the now all-too-familiar 'revolving-door' penetration of government regulation exploiting the absence of government-owned science advice focussed on the precautionary principle and the public interest.]

105. The current policy assurances provide little indication that the governance board will have the ability to identify and deal with new technologies and increasingly sophisticated methods of exploiting data.

106. With an absent inter-disciplinary cohort of scientific, legal and technological experts representing the public interest, regulatory power naturally relocates or defaults from democratic processes to technocratic and often captured institutions who cannot address greater complexity and navigate uncertainty in the public interest:

> '"New governance" techniques—principle-based regulation, management-based regulation, meta-regulation, risk-based regulation, and enrolment strategies — constitute the bulk of the innovative instruments in the re-regulatory neoliberal legal toolbox. These techniques destabilize the traditional state-centered, binding legal template that dominated the earlier roll-back neoliberal and pre-neoliberal legal regimes. They do so by granting regulated entities a degree of autonomy within loose regulatory frameworks. In the process, these techniques respect and often replicate the practices and norms that regulated entities have developed. They thereby relocate regulatory power from democratic processes to technocratic and often captured bodies, and, typically, encourage the state to recede from its former dominating position.'[58]

---

[57] Ishmaev et al. Ethics in the COVID-19 pandemic: myths, false dilemmas, and moral overload. Ethics and Information Technology (2021) https://doi.org/10.1007/s10676-020-09568-6

[58] Viljanen et al. Introduction: Imagining Post-Neoliberal Regulatory Subjectivities. Indiana Journal of Global Legal Studies. 2016:23:2;377-382

APPENDIX

Digital Identity Lobby Group Members