DIGITAL JUSTICE STRATEGY

- PRINCIPLES –

By Professor Julian Webb

There is no single accepted definition of digital justice; the term can be used in a variety of narrow and wider senses. In a narrow sense, 'digital justice' addresses the need to identify, and prevent harms being caused by digital technology, to allocate responsibility for harms actually caused, and provide accessible and equitable pathways for redress. This recognises that, as the World Economic Forum's White Paper, *Pathways to Digital Justice* (September 2021) acknowledges:

> *Emerging technologies pose prominent legal and judicial challenges, in particular: how to incorporate responsible use of new data-driven innovations into protections that encompass rights beyond just data privacy; how to replace outdated legal codes with frameworks that are fit for purpose in the current digital era; and how to address the lack of fair process in automated decision-making within the context of justice systems* (p.11).

But this 'corrective' view of digital justice addresses only the symptoms, not the causes of widespread *digital injustice.* Thus, TNL takes the position that, while a meaningful digital justice strategy must include the corrective view, it must also go further and treat digital justice as a matter of social justice, not just legal rights and privileges. For the purpose of this strategy therefore,

> **digital justice policy is defined as a range of initiatives designed to advance equality of access to digital technology; to prioritise the digital participation of people who have been traditionally excluded from and marginalised by technology, and to provide citizens with individual rights and remedies appropriate to the digital age.**

It recognizes the importance of infrastructure development and access, of digital literacy and of reliable, public, information to a functioning democracy. It values digital and non-digital forms of communication equally and fosters knowledge-sharing across communities and generations.

Digital justice strategy is thus complex. The embeddedness of technology in the social, economic and political fabric of our lives means that the risks of digital injustice are pervasive and potentially impact all areas of government policy and practice.

In response to that complexity, a national digital justice strategy must start from a set of high-level principles that will provide the basis for consistent and co-ordinated policy action. This will include a programme of legislative reform that will, over time, give continuing legal effect to these principles.

The following **nine pillars** state the baseline principles currently needed. The first three set key pre-conditions necessary for digital justice; the second three set a baseline of individual (soft) 'rights' – the idea being that these will require 'hardening-up' into legal rights through a range of legislative actions. The final three are more specific and focus on core government responsibilities in respect of their own functions, and position government as a responsible leader in delivering digital justice.

THE NINE PILLARS OF DIGITAL JUSTICE

1. Access to digital services is a right, not a privilege.

2. Key digital infrastructures should be owned and/or governed as public utilities.

3. Digital justice requires an educated and risk-aware population. Education in digital and information literacy is a key, continuing, government responsibility.

4. Data subjects own their own data.

5. Everyone has autonomy in respect of their technological choices.

6. No person should be discriminated against as a consequence of their technological choices.

7. The use of automated decision-making by governmental and public bodies to determine the rights, entitlements or liabilities of any person should be transparent and subject to human oversight and review.

8. Any government service proposing to use an artificial intelligence (AI) system to deliver or augment their services should ensure that it complies with current best practice in respect of ethical AI design.

9. The use of facial recognition systems or similar biometric-based technologies for law enforcement and related functions shall not be pursued by any government, public or statutory body unless and until a proper system of legal safeguards has been put in place that takes due regard of fundamental human rights.