DIGITAL JUSTICE MANIFESTO

A Call to Own Our Digital Future

Just Net Coalition

KEY PRINCIPLES

1. Data subjects must own their data – individually and collectively
2. Our data requires protection from abuse
3. We need the tools to control our data
4. Data commons need appropriate governance frameworks
5. Data protection, sharing and use require new institutions
6. Data-creating work ought to come with data rights
7. Data should be processed close to the point of its origin
8. Cross-border data flows must be decided nationally

KEY PRINCIPLES

9 Techno-structures need to be reclaimed as personal and public spaces

10 We should own our software and be able to control it

11 Key digital infrastructures need to be governed as public utilities

12 Techno-structures must be decentralised for open use, with interoperability

13 Global digital monopolies should be broken

14 Societies' datafication needs to be managed democratically

15 Digital standards must be developed by public interest bodies

16 The digital has to be governed in a local-to-global manner

PREAMBLE

We begin by reaffirming **'The Delhi Declaration for a Just and Equitable Internet'**. The present Manifesto builds on this Declaration and extends it.

A digital society is upon us

The emerging digital future is generally greeted with a mixture of positive anticipation, awe, helplessness and even horror. **Such a merely passive reaction to society's most powerful driving force is both dangerous and unnecessary**.

There is no time to lose in taming the power of the digital. We can either surrender our digital future, or we can take ownership of it. **But first we must understand what lies behind the digital**.

Industrialisation harnessed massive physical power from sources beyond those of people and animals, which transformed the processes of production. This is known as mechanisation. A digital economy and society is created by harnessing external (non-human) sources of 'intelligence power', in the form of immense data-based intelligence, which is revolutionising the forces of production. **This can be called the 'intelligencification' of socio-economic processes.**

Colonisation bore horrific witness to how industrial power coupled with imperatives of capital was almost impossible to resist or challenge by those subjected to it. Yet the **power of others owning detailed intelligence about us**, that is employed to generate unprecedented economic and political control, is perhaps worse than anything we have experienced so far.

Data, intelligence and techno-structures

Data must *inter alia* be recognised as a key economic resource. Currently, the resource of data gets globally appropriated at will; harvested without permission or recompense, and accumulated by data corporations for their exclusive use. **We must choose whether to allow corporations to own our data, or we, the people, should own it. The people, after all, are both the contributors and subjects of data**. Data corporations take advantage of the lack of any legal economic rights around data, to entrench their data practices as default law. Legal regimes are urgently required that affirm people's rights and ownership over their data – both individual and collective.

Digital 'intelligencification' was preceded and enabled by the spread of **networked software as the space, means and logic of our social, economic, political and cultural interactions and relationships**. The Internet was its first prototype. As the Internet's core model was based on intelligence at the edges and on open, public protocols, it spawned a technical and social evolution that many

believed would favour greater end-user control and decentralisation. Cloud computing – currently the dominant networked software model – has inverted this paradigm: **intelligence is now monopolised by a few global centres, based on corporate control of data and private standards**. The ubiquitous spread of Internet-based cloud applications enables the relentless collection of the most intimate and granular real-time data about us, the people. This is what builds the powerful autonomous intelligence behind the phenomenon of digital society.

At the centre of intelligent digital systems are a few global businesses – 'intelligence corporations', whose services are based on digital intelligence or artificial intelligence (AI). These corporations first connect, then coordinate, and ultimately control all actors and activities in any sector – from transport and commerce to health and education. **They become the 'brain' of every sector**. Global intelligence corporations **operate remotely through techno-structures of cloud computing**. Bypassing face-to-face human interactions, they thus avoid responsiveness and accountability, as well as legal and regulatory checks.

Taking back digital power

Reclaiming power from 'intelligence corporations' requires us to work on two main fronts. First, **wrest back ownership of our personal and collective data and intelligence**. These are the key sources

of digital power. And, second, **take sufficient control over the techno-structures** within which data and intelligence operate. These techno-structures spread wide and deep into society, controlling and exploiting everything they reach. Unlike in the offline world where socio-economic interactions mostly take place in public or quasi-public spaces, in the digital world they are all enclosed within privately owned techno-structures.

Yet, intelligent systems can operate productively even when their intelligence, as well as the key nodes and pillars of their techno-structures, are distributed and collectively owned. This would involve employing the best possibilities of entrepreneurship and competitive markets, combined with critically important non-market collective mechanisms. **Such alternatives must be shaped at the same time as the exploitative dominant models of centralised intelligence control are undone**.

The digital reshapes our social relationships and power structures so fundamentally that society's **data and intelligence governance requires a new digital social contract**.

In our determination and struggle **to enable people to own their digital futures**, we adopt the following principles towards a digital society that is just, equitable and sustainably productive.

People own their data and intelligence

1. Data subjects must own their data – individually and collectively:

Data about us, and intelligence about us, inherently belong to us – as individuals, and as communities. Such data could directly be about people, or about things owned by or associated with them. Political, constitutional, and legal frameworks, at both national and international levels, must recognise and enforce this basic principle of data and intelligence ownership.

2. Our data requires protection from abuse:

The international human rights regime must recognise the inextricable interconnection between people and their data, and articulate benchmarks for safeguarding personal and collective data. Strong constitutional and legal protections are required against abuse of personal and collective data and

intelligence, whether by corporations or the state. New laws and institutions that keep evolving to address emergent new risks are required for this purpose.

3. We need the tools to control our data:

The purpose of data and intelligence must not be to distinguish between people for unfair or discriminatory treatment, but to help and enable them to maximise digital benefits. Individuals and communities must be provided appropriate means to control their data, and apply it in ways best suited to their interests. Such means will be both individual and collective, requiring institutions that are adequate, agile and accountable. Institutional innovation in this regard will require well-regulated open markets ensuring competitive businesses, as well as new commons and public structures.

4. Data commons need appropriate governance frameworks:

Appropriate data commons and intelligence commons are required to be developed. But data and intelligence cannot simply be open access resources. To prevent their abuse, boundaries and protections are essential. Being specific to particular individuals or groups and communities, unchecked access to, and use of, data and intelligence commons bear the potential for harm. The ways in which data

actually gets employed by digital businesses, data and intelligence commons are akin to 'common pool resources' – subject to overuse, depletion, congestion, rivalry and pollution. Requiring regulated use, data and digital intelligence must be subject to 'common property regimes'. This calls for the development of necessary data and intelligence governance frameworks.

5. Data protection, sharing and use require new institutions:

Innovative and robust institutions are needed for sharing of data and intelligence in a protected and regulated manner. Data institutions, such as data commons, data trusts, data infrastructures, and fair data markets, must be developed. These should also involve mandated data sharing, as and where appropriate. Businesses and other entities have to be simultaneously provided with sufficient incentives, within a public interest framework, for them to collect the necessary data and process it into useful intelligence.

6. Data-creating work ought to come with data rights:

Specific economic groups that make marked contributions to, and are key subjects of, data in a particular sector or an 'intelligent system', should have corresponding special data ownership rights. These could be drivers on a taxi platform, traders on an e-commerce platform, farmers on an agri-platform or workers in data-producing jobs. These groups

must have primary economic rights – individual and collective – over the data they contribute. Such data constitutes the main value of the corresponding platform or intelligent system. Data-creating actors on a platform therefore have the right to participate in the governance of that platform, for example through adequate representation on the governing board. Alternatively, they may choose to pool their data to develop platform cooperatives, or a public or non-profit agency could help them to so organise.

7. Data should be processed close to the point of its origin:

In contrast to the current situation where digital activities on the ground are largely remote-controlled 'satellite operations' of a few global corporations, digital should have a pronounced localness and community control. Important data will need to be localised in many cases. If data is processed close to its point of origin, data subjects can have more effective control over their data. Necessary technical, policy and business models should be employed towards a local-to-global architecture of data and digital services. Technologies already exist for decentralised data control, and further innovations will emerge as society demands them.

8. Cross-border data flows must be decided nationally:

The data-owning national community must determine the terms on which cross-border flows of data may take place. Irrespective of its physical

location, data should be subject to the primary jurisdiction of its country of origin. As personal data is an extension of one's person-hood, so also community data is an extension of community identity and being. Such primary jurisdiction involves not just privacy protections but also economic rights and ownership. Agreements among countries are required to mutually recognise, and help apply, primary jurisdiction over data – involving social, political and economic rights – of the country and community of origin of data. Regional groups that manage to enter such inter-country agreements may gain mutual benefit from common data and digital spaces.

People have rights to their digital techno-structures

9. Techno-structures need to be reclaimed as personal and public spaces:

Networked software or cloud applications form the digital space, and the body of digital systems. These may be termed as the key digital techno-structures. They are currently almost entirely centralised and owned by a handful of corporations. Some, like those running heart pacemakers or mobile phones, penetrate deep into our personal realms; and some, like social networking, search, and

transport applications, are analogous to what in the offline world are public spaces and structures, such as public streets, libraries and infrastructural services. Digital techno-structures' personalness and publicness, as applicable, must be reclaimed from the existing state of their complete, end-to-end, corporate ownership and control.

10. We should own our software and be able to control it:

People must fully own, and be able to control, the software they install in their personal or collectively owned equipment. Technology Protection Measures are incursions upon people's basic rights. People should have the right to own, break-into, modify or remove, as they deem fit, whatever technical artefacts that exist within their personal or collective realms. This is a fundamental element of digital self-determination.

11. Key digital infrastructures need to be governed as public utilities:

In the physical world, non-personal, social and economic spaces and structures are divided between being public and belonging to private businesses. Infrastructure is normally public, or quasi-public, over and around which businesses may undertake their private activities. Digital spaces and structures require a similar arrangement. Key monopolistic digital infrastructures should be governed as

public utilities, even if they are provided by private businesses. This includes, as appropriate, computing platforms, search engines, social networks, email services, basic security systems, payment services, and e-commerce platforms.

12. Techno-structures must be decentralised for open use, with interoperability:

Digital power can be redistributed by decentralising the techno-structures of connectivity, software, Internet, cloud computing, and AI applications, while mandating interoperability. Such decentralisation is useful even where it entails some degree of immediate loss of efficiency. Apart from being fairer, decentralised digital power is more sustainably productive in the long term. Decentralised and open digital architectures include open community networks, open source software, an open and neutral Internet, open and community data, and open and community AI. These can and should involve appropriate business models and entities. Any such open system must however duly protect the data and digital intelligence of the people and communities concerned, and affirm their right to self-determination.

13. Global digital monopolies should be broken:

National and international competition regimes, that are adequate to the new digital realities, must break up vertically and horizontally integrated global

digital structures. These regimes should aim at *ex ante* open, competitive and innovation-supporting digital market structures, and not just narrowly construed *ex post* consumer welfare that looks only at availability and price of goods and services. The focus should be on cutting problematic links in data and intelligence value chains that underpin and promote digital monopolies. It may for instance be considered, where appropriate, to separate businesses that directly provide digitally-enabled services to consumers, and collect their data, from businesses devoted specifically to technical services, and general data processing and digital intelligence services.

The digital must be governed democratically, from local to global

14. Societies' datafication needs to be managed democratically:

Areas facing or undergoing datafication and 'intelligencification' require a three-way classification. Many kinds of datafication and 'intelligencification' are just not desirable, whatever their touted benefits. In other areas, while potentially useful in the long run, these processes may call for deliberate slowing

down and appropriate governance, to deal with the possibilities of considerable short- to mid-term harm. Such harm could range from livelihood disruptions to requirements of significant behavioural and cultural shifts that can be disorienting. Where datafication and 'intelligencification' are evidently beneficial to undertake right away, people, and their representatives, should be in control of their implementation. These processes tend to have strong unanticipated social consequences and must take place on democratically determined terms. A global human rights framework on data and intelligence governance should incorporate such a classification and the corresponding due diligence.

15. Digital standards must be developed by public interest bodies:

A major factor behind the current end-to-end digital control by a few digital corporations is the privatisation of digital standards development and non-enforcement of interoperability. We must reclaim development of key digital technical standards exclusively by public interest bodies, and ensure strict compliance with such standards. These bodies should be based on public-interest oriented expertise, under the appropriate oversight of people's representatives. Standards-developing bodies should uphold the highest public and professional standards, be neutral and not aligned to any specific corporate or political interests, and fully eschew conflicts of interest.

16. The digital has to be governed in a local-to-global manner:

Digital platforms provide services that have traditionally been largely developed and governed locally – like communication, media, commerce, transport, hotels, health and education. Having now become intelligence-driven does not necessarily mean that these services shed their localness. The required new digital, data and intelligence governance structures and institutions will mostly be at national or local community levels, while some could be global. National polities still remain the anchors of self-determination and sovereignty of the people. Appropriate global governance of the digital should promote national and local digital economies. It ought to ensure that competitive and open global technical services are accessible locally – including by local digital businesses – on fair and regulated terms. Digital governance must aim at a complete break from the current vertically-integrated global digital models – from concentrated intelligence or 'brain' centres in one or two countries of the world, right down to the last tiny 'nerves' that seek to control the smallest activity everywhere in a digital economy and society. A new digital model that is local-to-global must be shaped, which supports localness and furthers democratic self-determination, without compromising on the important benefits of the globalness of the digital.

We propose these principles as the basis for a new governance architecture of a digital society that is just and humane.

DEVELOPED BY JUST NET COALITION, NOVEMBER 2019

Write for endorsement of the manifesto,
further information or comments to

info@justnetcoalition.org