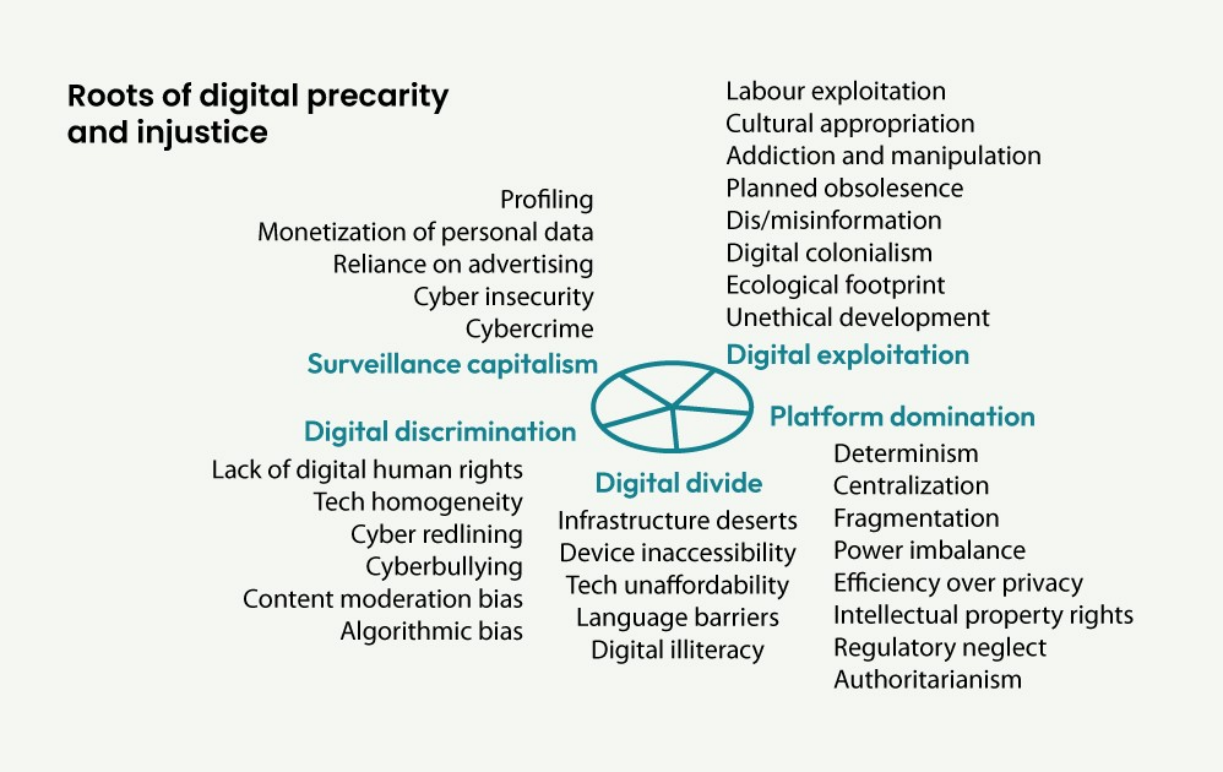
Knowledge base

Digital precarity and injustice



Digital divide

The digital divide refers to the unequal distribution of access to digital technologies and the internet, often along socioeconomic and geographic lines.

It creates gaps between those who have access to information, resources, and opportunities offered by digital technologies, and those who do not. This divide perpetuates existing inequalities and limits opportunities for those who are already marginalized or disadvantaged, such as low-income, seniors, rural and remote communities, and people with disabilities.

Five traits of the digital divide include *infrastructure deserts, device disparity, tech unaffordability, language barriers,* and *digital illiteracy*.

- **Infrastructure deserts**
  The systemic limitation or insufficiency of access to digital infrastructure across

regions, municipalities, or neighbourhoods, such as low broadband connectivity in rural and remote communities.

- **Device inaccessibility**
  The inadequate or uneven distribution of access to digital devices that are necessary to participate in the digital world, such as computers, smartphones, or tablets.
- **Tech unaffordability**
  The high cost of digital technology hardware and software, internet access, and other digital resources that limit opportunities to contribute to our increasingly digital society and economy.
- **Language barriers**
  The lack of digital content and services in languages other than English that make it difficult for non-native speakers to access information and participate in the digital world.
- **Digital illiteracy**
  The lack of appropriate, affordable, or open access to education and digital skills training that are necessary for employment, entrepreneurship, and confident participation in our increasingly digital society and economy.

Digital discrimination

Digital discrimination refers to the unfair and unjust treatment of individuals or groups in digital spaces online. It is often rooted in existing social inequalities and can amplify discrimination and prejudice in the real world offline for many diverse communities, such as 2SLGBTQIA+, Indigenous, Black, and other people of colour.

Six examples of digital discrimination include *lack of digital human rights, tech homogeneity, cyber redlining, cyberbullying, content moderation bias,* and *algorithmic bias.*

- **Lack of digital human rights**
  The absence or violation of fundamental human rights in the digital realm, such as privacy, freedom of expression, access to information, and non-discrimination.
- **Tech homogeneity**
  The overrepresentation of a narrow demographic (i.e., white males from affluent backgrounds) in the digital technology industry that can lead to homogeneous thinking, biased product development, and lack of innovation and creativity in the industry.
- **Cyber redlining**
  The denial of access to digital services and resources based on race, income,

geographic location, or other factors which exacerbate existing inequalities and discrimination leading to the perpetuation of social and economic injustices.

- **Cyberbullying**
  The use of digital technologies to harass, intimidate, or bully individuals or groups based on gender, sexual orientation, race, religion, class, income, or other factors.
- **Content moderation bias**
  The systemic censorship, discrimination, or unfair treatment towards certain groups or types of content by human moderators or algorithms used for moderating content on digital platforms, typically related to social justice movements or political speech.
- **Algorithmic bias**
  The perpetuation of existing patterns of discrimination or unfair treatment in the data used to train machine learning algorithms and artificial intelligence systems.

Surveillance capitalism

Surveillance capitalism refers to the collection and monetization of personal data and using it to predict and influence individual behaviours and preferences. It involves the collection, analysis, and sale of large amounts of personal data by corporations, often without the knowledge or consent of individuals. Considerable trust, security, and privacy issues arise when surveillance data is not sufficiently stewarded.

- **Digital profiling**
  The collection and analysis of digital data to create profiles of individuals or groups, often for targeted advertising, content delivery, or surveillance. This can include tracking interactions with social media and search engines, location data, and other personal information which can then be used to assume or predict a person's preferences, interests, and behaviours. Digital profiling can contribute to algorithmic bias and discrimination, filter bubbles, as well as privacy violations and the erosion of digital rights.
- **Monetization of personal data**
  The collection and sale of the personal data of individuals or groups, often for profit, which can lead to privacy violations and the exploitation of personal information.
- **Reliance on advertising**
  The growth and proliferation of advertising-based business models among online platforms, where advertising revenue is the primary or only source of income. This business model incentivizes the collection of personal data to target ads to individuals and groups.

- **Cyber insecurity**
  The inadequate or uneven distribution of access to digital systems, networks, and devices that protect against cybersecurity threats and attacks. This can lead to the loss of sensitive information, data breaches, identify theft, financial fraud, surveillance and censorship, and other negative infringements on digital rights and freedoms.
- **Cybercrime**
  Illegal activities committed in digital spaces with the intention of stealing information, disrupting services, or extorting money. Examples include hacking, phishing, identify theft, automated robocalls, and online scams.

Digital exploitation

Digital exploitation involves the use of technology to disregard, manipulate, or oppress vulnerable individuals and groups for financial gain.

- **Labour exploitation**
  The unethical or illegal labour practices that often take place in digital work environments. Examples include workers that are underpaid, overworked, lack job security and benefits, are subjected to poor working conditions, have limited opportunities for advancement, and experience wage theft. Digital labour exploitation disproportionately affects vulnerable workers, including women, migrants, and gig workers.

- **Cultural appropriation**
  The unauthorized use of cultural protocols, materials, knowledge, expressions, or artifacts that belong to a particular group or community for commercial or personal benefit, without proper acknowledgement or compensation to the rightful owners. This can lead to the erasure of the original cultural context and meaning, economic exploitation, and perpetuation of power imbalances in the digital world.
- **Addiction and manipulation**
  The harmful or unethical use of gamification, persuasive design, and other psychological techniques to keep users engaged with digital technologies and services, often leading to compulsive use and addiction. This can be particularly harmful to children as they are often less capable of understanding the risks and are more vulnerable to manipulation.

- **Planned obsolescence**
  The practice of intentionally designing digital hardware and software to quickly become outdated, wear out, or become unusable after a certain period of time. This forces users to purchase newer versions or upgrades to access the latest features and functionalities, creating a cycle of dependency and consumption that drives profits at the expense of the environment and consumer wallets.
- **Disinformation**
  The intentional spread of false or misleading information with the aim to deceive or manipulate people's beliefs or behaviours. Examples include fake news, political propaganda or hoaxes, malicious attacks on individuals or organisations by bots and fake social media accounts, and deepfakes or manipulated media.
- **Misinformation**
  The spread of false or misleading information without necessarily having the intent to deceive, often due to a lack of accurate information or understanding. Examples include inaccurate news reports, echo chambers, and clickbait.
- **Digital colonialism**
  The imposition or domination of digital technologies, platforms, and information that maintain or exacerbate inequitable relationships established through colonialism, often with little regard for the rights, cultures, or well-being of those affected. Digital colonialism can take many forms, such as the erasure or extraction of digital data from Indigenous communities, the use of digital surveillance to monitor and control Indigenous movements and resistance, and the propagation of Western cultural values and norms through digital platforms.
- **Ecological footprint**
  The increasing environmental impact of digital technologies and the internet, including unsustainable resource consumption, e-waste generation, and carbon emissions that contribute to climate change, pollution, and other environmental issues.
- **Unethical development**
  The development of new technologies that are deemed partially or entirely unethical due to their negative impacts on individuals, communities, and the environment. Examples include racial bias and discrimination in facial recognition and privacy violations in biometric tracking.

Platform domination

Platform domination refers to the consolidation of power by a small number of dominant platforms in the digital landscape. It can stifle competition, restrict consumer choice, reduce the diversity of viewpoints, and erode privacy and digital rights. It can also lead to the concentration of wealth and power in the hands of a few individuals or corporations, thereby amplifying existing power imbalances and contributing to digital inequality and injustice.

- **Determinism**
  The belief that digital platforms and technologies are inherently a force for good or the main driving force behind innovative social change. This can result in the imposition of technological solutions on communities without consideration of their needs and perspectives or the ways other social, economic, political, and environmental factors shape the use and development of technology.
- **Centralization**
  The concentration of power, control, and ownership of digital infrastructure, information, and services in the hands of a small number of large corporations or entities. This leads to the exploitation of users through monopolistic practices, lack of competition, reduced privacy and security for users, and limited access to information and resources.
- **Fragmentation**
  The lack of integration and interoperability between different digital platforms, systems, or devices. This results in limitations for users to access and use digital services or products, and can amplify in exclusion, discrimination, and inequitable distribution of digital benefits and opportunities.
- **Power imbalance**
  The inequitable distribution of power between platform operators and the users. As operators amass greater control and influence over the users' personal actions and data, users have become increasingly reliant on the platform, creating a power imbalance that can be exploited for profit.
- **Efficiency over privacy**
  The collection and use of user data by digital platforms to maximize efficiency and profit at the expense of user privacy and control over their personal information. This approach is common among many tech companies and can result in a lack of transparency and accountability around data collection, storage, and sharing practices.
- **Intellectual property rights**
  The concentration of intellectual property rights in the hands of a few large corporations limits access to digital resources and impedes innovation, particularly

in developing countries. The lack of ownership and control over their own content also adversely impacts individual users.

- **Regulatory neglect**
  The failure of governments and regulatory bodies to adequately oversee and regulate the activities of digital platforms, resulting in a lack of accountability, transparency, and protection for users. Examples include inadequate data protection laws, lack of enforcement of antitrust laws, and failure to address harmful content on social media platforms.
- **Authoritarianism**
  The use of digital technologies by governments or other powerful entities to exert control and restrict individual freedoms through surveillance, censorship, and other forms of repression. It can also refer to the consolidation of power by a small group of individuals or entities who control key digital platforms and use them to manipulate public opinion or restrict access to information.