# Futures of Data Ownership

Defining Data policies in Canadian Context

By Vinit Soneji | Strategic Foresight and Innovation ‘23

**Futures of Data Ownership: Informing Data Policies in Canadian Context**

**by**

**Vinit Soneji**

Submitted to OCAD University in partial fulfillment of the requirements for the degree of Master of Design in Strategic Foresight & Innovation Toronto, Ontario, Canada, May, 2023©Vinit Soneji, 2023

# Creative Commons License

# Abstract

The importance of data is increasing along with its inflation in our world today. In today's world, data is becoming the primary source for innovation, knowledge, insight, and a competitive and financial advantage in the race of information procurement. This interest in acquiring and exploiting data and the current concerns regarding the privacy and security of information raises the question of who should own the data and how policies can preserve data ownership. There is a growing awareness that companies benefit disproportionately from collecting and selling personal information, driving the desire for greater individual control of personal data. As technology progresses exponentially, there is a dire need to regulate Tech organizations.

With the increasing use of personal data by tech companies, data privacy and ownership concerns have become more significant in today's society. Although governments worldwide have introduced privacy regulations to protect citizens' data, there is still a need for policies and legislation that safeguard citizens' rights, allow consumers to control their data, and implement strict measures in case of data breaches or violation of data rights.

The research project "Futures of Data Ownership - Informing Data Policies in Canadian Context" aims to explore emerging technological shifts and promote ethical use and data protection by developing data policies that consider the Canadian context. The research will employ primary and secondary research methods, including horizon scanning, semi-structured interviews, and a literature review, to inform policy and strategy development. In conclusion, the research project informs potential policies and legislation that regulate tech organizations and protect data ownership, ensuring a secure and trustworthy digital future for all.

# Acknowledgements

I am grateful for this land, the traditional territory of many nations including the Mississaugas of the Credit, the Anishnabeg, the Chippewa, the Haudenosaunee and the Wendat peoples, and all the life that it has held, holds, and will hold.

To Dr. Michele Mastroeni , my primary advisor. Thank you for your steady faith in my process and for supporting me with your always considerate and analytical perspective. Under your guidance I got to know myself better, in the ways that I learn best. This project could not have been completed without your support and guidance. I am incredibly fortunate to have had you as my advisor.

To my family, my Mom and Dad and my sisters, my life mentor and support Shruti Soneji. My friends namely Dr. Aanchal Bhandari, Neel Dave and Vaishnavi Joshi. I express my gratitude for giving me emotional and mental strength and having faith in me throughout the journey. I am simply grateful for your presence.

To my friends from SFI cohort namely Javier, Rhea, Kassie, and Tanya I express my gratitude for collaborating with me, lending a ear, and providing unwavering support during the course of my research. Our discussions have aided me in gaining clarity and developing the courage to persist through the challenges, uncertainty, and discomfort that come with the research process. As well as, to everyone in my SFI cohort who brought impeccable knowledge and discussions.

To REF Squad at EcampusOntario. I am grateful to you for fostering an atmosphere that encouraged creativity, discussions, and trust, where I could effectively apply the knowledge gained from my SFI and broaden my horizons. Especially, Dr. Alex Hughes, thank you for listening to me and answering my silly questions.

## To all these great people, I am forever in your debt.

# Contents

## Tables and Figures

# Introduction

Why is data privacy important?

What are the drivers pushing for effective privacy policy?

Who owns your data?

# Glossary

**Personally Identifiable Information (PII):** Data that is unique or close to unique for a particular individual. This is usually defined in policy and regulation and can include things that you might not expect — like your IP address, date of birth and workplace.

**Person-Related Data:** Data that relates to a person but doesn't fall under PII. This could be anything related to their personhood, including interests, beliefs, locations, on line and offline behaviors and activities.

**Proprietary and Confidential Data:** Data deemed as sensitive for contractual or business-related purposes. Its release would endanger a business or other legal relationship or agreement.

**Big tech companies:** A term used to describe the largest technology companies in the industry.

**Data versus information:** Data is raw. It simply exists and has no significance beyond its existence (in and of itself). It can exist in any form, usable or not. It does not have meaning of itself. In computer parlance, a spreadsheet generally starts out by holding data. Information [...] is data that has been given meaning by way of relational connection. This 'meaning' can be useful, but does not have to be. In computer parlance, a relational database makes for information from the data stored within it." (Bellinger, et al., 2004, paras. 4-5)

**Emerging Shifts:** Emerging shifts or trends are a combination of weak signals that might grow in scope and scale in the future.

Strategic Foresight: Strategic Foresight is an organizational, social, and personal practice that allows us to create functional and operational views of alternative futures and possibilities" (The Futures School, 2015, para. 1)

**Scenarios**: Possible visions of the future used for strategic decision making (Finch & Casasbuenas, 2020, para. 3)

**Data Controllers:** The UK GDPR defines a controller as: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**Data Processors:** The UK GDPR defines a 'processor' as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

**Data Trusts:** Data trusts are a tool for formalizing markets, supply chains, and governance mechanisms in ways that keep everyone involved accountable to public expectations, in order to legitimize digital transformations.

**First-party data:** First-party data is individual data collected with consent and is in direct relationship with the customer. This type of data is not shared (eg: Email, phone number, purchase history)

**Second-party data:** Second-party data is individual data collected with consent and is in in-direct relationship with the customer. It usually it is data linked to an individual and shared with only trusted partners (eg: website activity, customer feedback)

**Third-party data:** Third-party data is aggregated data that may be collected with consent and is in in-direct relationship with the customer. This type of data is shared with many companies (eg: income, education, websites visited)

**CPPA:** Consumer Privacy Protection Act. A new data privacy policy in Canada

**Interoperability:** The ability of computer systems or software to exchange and make use of information.

# The story

The importance of data is increasing along with its inflation in our world today. A recent study by Cisco found that 86% of consumers “care about data privacy” and want more control, 79% are willing to spend time and money to protect data, and almost half of consumers “have switched companies or providers over their data policies or data sharing practices.” (Goswami, 2021) In this significant data era, data is becoming the primary source for innovation, knowledge, insight, and a competitive and financial advantage in the race of information procurement. This interest in acquiring and exploiting data and the current concerns regarding the privacy and security of information raises the question of who should own the data and how policies can preserve the ownership of data. There is growing awareness that companies benefit disproportionately from collecting and selling personal information, driving the desire for greater individual control of personal data. (Specht, 2019)

In recent years, there has been a growing concern about the impact of social media and technology on our lives, particularly in regards to data privacy. Eye-opening documentaries like The Social Dilemma, The Great Hack, and Coded Bias have highlighted the extent to which tech companies collect and use personal data. These documentaries showcase the trade-off between our personal data and the social platforms we use every day.(Amnesty International, 2021) (Seetharaman, 2019)

Governments around the world have introduced privacy regulations to protect citizens’ personal data. The General Data Protection Regulation (GDPR) is a comprehensive data protection law that was introduced in the European Union in 2018. (Data Protection in the EU, 2021)  The California Consumer Privacy Act (CCPA) is another privacy regulation that was introduced in the United States in 2020. The Brazilian General Data Protection Law (LGPD) is another recent privacy regulation that was introduced in Brazil in 2020. Multiple governments of the world have started to form privacy policies for multiple reasons.

There is a need to define policies and legislation that protect citizens, allow consumers to control their data, and introduce strict measures in case of data breaches or violation of data rights. Currently, PIPEDA (Canada’s data policy) entails that organizations that collect, use, or disclose personal information must obtain individuals' consent, limit their collection, use, and disclosure of personal information, provide individuals with access to their personal information, and protect the security of personal information.(Office of the Privacy Commissioner of Canada, 2019) The research studies data ownership and sovereignty, the intricacies of data policies, and inform data policies for Canadian citizens. The research will shed light the factors that affect the problem space of data privacy policies. The research uses design methods and principles, and tools and frameworks from the strategic foresight domain.

This MRP uses secondary and primary research methods to gather information about the domain as well as emerging shifts that are likely to disrupt the status quo. The problem framing, analyzing, synthesizing, and solving will be conducted through understanding human factor, understanding major stakeholders, casual layered analysis, mapping the flow of data, and conducting interviews. The outcome of this MRP would inform strategies and scenarios that are necessary to mitigate the problem of data ownership. As technology continues to progress exponentially, defining policies and legislation that regulate tech organizations and protect data ownership will be critical in ensuring a secure and trustworthy digital future.

## Objectives

This research aims to achieve the following objectives:

1. Trace the origins and evolution of data privacy.

2. Define the insufficiencies of the current system

3. Explore new ways of thinking about ethical use of data that are on the horizon

4. Recommend decision making principles for policy and strategy development

## Directed Audience and Stakeholders

The purpose of this research is to provide a futuristic perspective to the Canadian Radio-television and Telecommunications Commission (CRTC), the Canadian Digital Service (CDS), the Competition Bureau's Digital Enforcement Branch (CCCS), and the Office of the Privacy Commissioner of Canada (OPC), to help them facilitate decision making and form policies for their ethical use of data. Additionally, the research could be used by think-tanks, NGOs and other decision makers in the space of data privacy. The study highlights the current picture of data collection, utilization, and dissemination through various platforms and channels. Additionally, it underlines the potential future risks and benefits of data that are likely to surface. Moreover, it proposes multiple strategies and frameworks to regulate data practices and establish a system of checks and balances towards ethical data use.

The study recommends that these regulatory bodies establish a system of checks and balances to monitor data practices and prevent any unethical usage of data. In conclusion, this study is directed towards the decision makers to provide them with a proactive approach to regulate data practices and promote ethical data use. By implementing the recommended measures, these regulatory bodies can ensure that data is utilized in a responsible and ethical manner, thus mitigating potential risks and maximizing the benefits of data in the future.

# Research Question

## How might we inform data privacy policies in Canadian society that promote the protection of consumer privacy and ethical use of data in view of emerging shifts?

**1.Inform:** The goal of this research is to cohesively inform data privacy policies by understanding the current data privacy policy in Canada(PIPEDA), inspirational policies(GDPR) and changes across the world to provide strategies and recommendations.

**2.Canadian Society:** The research is only limited to the Canadian context. The research is centered on dynamics and changing landscapes of the data world viewing them through the lens of Canadian Society. Additionally, the research considers the population, systems, data rights in Canada.

**3.Consumer Privacy:** The research takes into account the harms and exploitation of an individual with respect to their personal information, while also addressing the need for businesses to collect, use or disclose personal information for reasonable and appropriate purposes.

**4.Ethical use of Data:** Collection of data and protecting it is only one part of the major problem. The ethical use of data describes the collection, dissemination and use of data by third-party seller.

**5. Emerging Shifts:** The term 'emerging' describes changes that are on the horizon. These changes are currently at their initial stages and it is uncertain how they might grow in the future.

# Report Structure

The report is divided into five chapters, each with a specific focus on different aspects related to the project. The **first chapter** provides an overview of the project and sets the tone for the rest of the report. The **second chapter** explores how data has become the primary driver of decision making in the current era, starting with the rise of consumer culture post-World War II and the impact of the digital revolution. The **third chapter** examines the current state of data policies in Canada, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and Consumer Privacy Protection Act (CCPA, Bill C-27), and identifies areas for improvement. The **fourth chapter** explores three distinct scenarios for data ecosystems, and a theoretical framework is presented based on core values and guiding principles that could form the foundation for future work related to data privacy or policy initiatives. The **fifth and final chapter** presents a theoretical framework that combines the strengths of the current state with the most promising elements of the alternative states, including a set of core values critical for creating a sustainable and responsive data ecosystem, and a set of guiding principles for developing data policy initiatives that prioritize these values

# Methodology

This section describes how information was gathered for the design thinking process. This research includes both primary and secondary information sources. It draws from three sources of information: literature review, horizon scan, and semi-structured interviews.

**Literature review:** A literature review was conducted to explore the state of the art and the drivers influencing the more extensive system. The literature review included academic papers, journals, books, news articles, and podcasts. The exploration included the following topics: the data economy, data sharing policy making, data policies worldwide, surveillance technologies, the rise in consumerism, the Canadian landscape, web 3, and other rising technologies in the data ecosystems. Signals, drivers and credible arguments were compiled to form trends. Signals and credible information from the literature review were compiled by analyzing patterns, concerns and potential significant directions in the data era. From there, the interconnections between signals and their positioning within the more extensive system could be evaluated. Due to inadequate responses in the interview, a stronger emphasis was given to the literature review to collect information and inform data privacy policies.

**Semi-structured interviews:** Conducting personal interviews allows us to understand the subject area's perspectives and design human-centred recommendations that address stakeholder needs. The literature review uncovered that open data research tends to be expert-driven, focusing on data providers' perspectives. This is because the average citizen tends to experience open data through secondary distillations and is often unaware of the original data source. This research aims to include professionals who provide the data and urban stakeholders who use it in their domains. An initial list of interview participants was identified through online research. Participants were added to the list through snowball sampling as participants recommended additional candidates. Four remote semi-structured interviews were conducted with Government officials involved in data privacy, academics, data and technology specialists, researchers, and urban stakeholders. Due to time constraints and lack of interview participations, a stronger emphasis was given to the literature review. Each participant was asked a set of predetermined questions. The interview questions were designed according to the following structure: examining the present, exploring possible futures, and bridging the gap between the present and their preferred future scenario. The audio of each interview was recorded and fully transcribed. In the semi-structured interviews, various themes were identified, which further added an immense value in analyzing trends and suggesting privacy-centric measures. This research was approved by the OCAD University Research Ethics Board.

**Horizon scanning** is a method used in strategic foresight to gather evidence of possible future developments that could change the current system structures (Cuhls, 2019). Evidence from the presence of possible or emergent future change is more commonly known as a weak signal. For this project, the horizon scan consisted of looking for weak signals in various mediums such as news sources, social media platforms, science fiction, literature, academic research, interviews, and documentaries. Over two hundred signals were collected, including evidence of future innovations, data practices, values, and ways of working that might influence data privacy in Canada. The weak signals were organized using the STEEP-V framework, a strategic foresight method ubiquitously used in horizon scanning (Richardson, 2017). The STEEP-V framework categorizes weak signals by their potential social, technological, environmental, economic, political, and values-based impacts. From there, the interconnections between signals resulted in trends and potential solutions and frameworks.

**Causal Layered Analysis (CLA)** The core framework and approach to analysis in this study relied heavily on Sohail Inayatullah's Causal Layered Analysis (CLA). This is a foresight method that provides a structure to frame and enable the synthesis of complex issues where system levels could be looked at through varying dimensions. Inayatullah (2004) explains that the use of the CLA is meant to provide a deep understanding of contextual problems to create transformative, authentic, alternative futures. This defining feature of the CLA is that it is 'concerned less with predicting a particular future, and more with opening up the present and past to create alternative futures' (Inayatullah, 2004).

“You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete.”

- Buckminster fuller

# Understanding the past: How did we get here?

How did it start?

What is data econonomy?

How does the idea of consumerism culture play a role in data privacy?

# Rise in Consumerism Culture

The post-World War II era witnessed significant changes in the world order that contributed to the emergence and entrenchment of consumer culture. The expansion of markets, both domestically and internationally. (Higgs, 2022) The growth of mass media and advertising allowed for the creation of new markets and the targeting of new consumer segments while establishing global trade networks facilitated the exchange of goods and services across national borders (Lury, 2011). The growth of consumerism further fueled these developments as a way of life, emphasizing the importance of consumption and materialism to achieve happiness and social status (Campbell, 1987). This was reflected in the rise of consumer-oriented lifestyles, such as suburban living and the adoption of new technologies and products, which became an essential aspect of modern identity (Schudson, 1984). The changes in the geopolitical world also contributed to the rise of consumer culture. The post-war era was characterized by a shift towards liberal democratic values and establishing a global capitalist system, prioritizing economic growth and individual freedom (Harvey, 2005). This created a favourable environment for the growth of consumerism, which was seen as a critical driver of economic growth and individual prosperity.

To navigate the shift in consumption habits that lies ahead, we must examine and learn from the history of our consumer culture. Through a thorough literature review of the behaviours, geopolitical nature, and the emergence of new economies post-World War II, "Takeaways from Consumer History" have been synthesized. These lessons highlight the role of emergent consumerism in the lives of the average person in Western civilization and provide insight into consumer culture's function with a nation's economy and prosperity. While these lessons are not universal truths, they reflect the trends that developed as society industrialized. Below are the five key learnings from the consumer culture that can inform our understanding of consumption practices and their impact on society.

**1. Consumer spending can drive economic growth:** Consumer spending is a significant component of gross domestic product (GDP), and an increase in consumer spending can stimulate economic growth (OECD, 2020). Consumer culture can have a positive impact on the economy of a nation.

**2. The rise of consumer culture has led to global economic integration:** The growth of consumer culture has facilitated the expansion of global trade and economic integration, with countries specializing in producing certain goods and services and engaging in trade to meet consumer demand. This has increased prosperity for some countries and challenges such as job loss and inequality (World Economic Forum, 2020).

**3. Consumer culture can contribute to income inequality:** The benefits of consumer culture are not evenly distributed, with some individuals and groups benefiting more than others (Stiglitz, 2012). This can contribute to income inequality within and between countries, negatively impacting social and economic outcomes.

**4. Consumer culture can have environmental consequences:** The production and consumption of goods and services can negatively impact the environment, including climate change, pollution, and resource depletion (IPCC, 2018). This can have long-term economic consequences, including the depletion of natural resources and the costs associated with environmental damage.

**5. Consumer culture can lead to unsustainable levels of debt**: Pursuing consumer goods and services can lead to unsustainable levels of debt for individuals and households, which can negatively impact financial stability and overall economic growth (Goodwin et al., 2018, p. 20). Consumer culture needs to be balanced with responsible financial management.

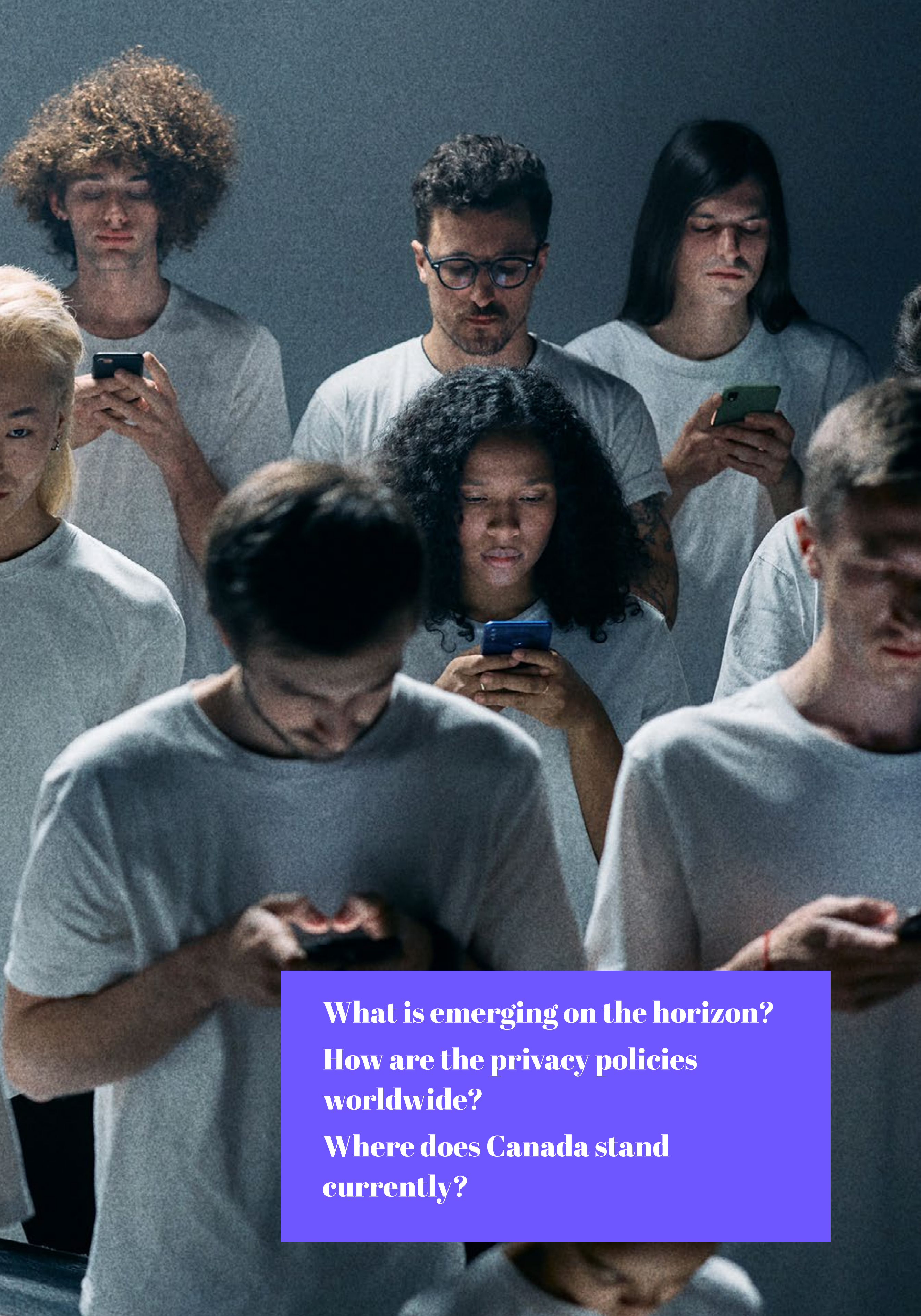
In conclusion, consumer culture positively and negatively impacts a nation's economy and prosperity. By understanding these key learnings, we can work towards a more sustainable and equitable economic system that balances the benefits of consumer culture with responsible management of economic and environmental resources. In today's age, technology and data have become crucial aspects that have reshaped societal values and brought about the Fourth Industrial Revolution. The convergence of physical, digital, and biological worlds has created promise and peril, forcing us to rethink how countries develop, how organizations create value, and even what it means to be human. The consumption culture is not restricted to physical products but also digital services, infrastructure, and sometimes hybrid. While technology presents an opportunity to create an inclusive, human-centred future, it also requires focusing on consumer mindsets, changing and shifting behaviours, and protecting citizens from physical challenges and data-driven harms and threats.

# Rise of Data Capitalism

The rise of consumer culture, driven by the widespread adoption of digital technologies, created a fertile ground for data capitalism. Personal data has become a valuable business asset and is exploited for financial gain. Data capitalism, commonly known as surveillance capitalism, is the unilateral claiming of private human experience as free raw material for translation into behavioural data. (The Rise of Data Capitalism - Trinità Dei Monti, 2021) It is an economic system in which personal data is seen and conceived as a source of profit. Surveillance capitalism arose and peaked when advertising companies understood the possibilities of using personal data to target consumers more effectively. (The Rise of Data Capitalism - Trinità Dei Monti, 2021) Digital platforms have mastered the ability to provide the exact product, service or offering a user wants due to personal data collection and insights from this exchange. This heightened level of personalization has provided users with the tool or offering to use at the exact contextual time needed, making life 'easier' and leading to instant gratification. In this context, instant gratification refers to the expectation of immediate fulfillment without delay (Taubenfeld, 2017). This exchange has perpetuated users' reliance, addiction and dependence on these platforms to maintain a convenient lifestyle, thus further reinforcing the power that specific platforms hold over those who use them (Telbis, 2019).

Newly available data sources have dramatically increased the quantity and variety of available data. Our expanding sensor-based society now includes wearables, smart home devices, drones, connected toys and automated travel. Sensors such as microphones, cameras, accelerometers, and temperature and motion sensors add to an ever-expanding list of our activities (data) that can be collected and commodified(Holloway, 2019). Shoshana Zuboff's latest book, The Age of Surveillance Capitalism, suggests that our emerging sensor-based society will make surveillance capitalism more embedded and pervasive. The rise in data collection and data collection technologies raises considerable concern about regulation.

# The Present: What is happening now?



What is emerging on the horizon?

How are the privacy policies worldwide?

Where does Canada stand currently?

# Emergence of Privacy Policies

The growing prevalence of data breaches, cyberattacks, and online fraud has become a significant concern for individuals, businesses, and governments worldwide. As more personal information is collected and stored online, the risk of this information being stolen or misused by hackers and cybercriminals has increased. This has led to a growing demand for greater protection of personal data. In addition, the increasing use of personal data by companies and governments has raised concerns about privacy violations and the potential misuse of data. With the rise of big data analytics, companies can collect and analyze vast amounts of data about individuals, including their online behaviour, shopping habits, and personal preferences. This has led to concerns about how this data is being used and whether individuals have adequate control over their personal information.

The Cambridge Analytica scandal, where 87 million Facebook users had their personal data was accessed without consent for specific political use, fuelled concerns about data ownership. The scandal was seen as a dystopian reality of psychological manipulation where people felt taken advantage of (Berghel, 2018; Isaak & Hanna, 2018). As the public has become more aware of these issues, there is seen a growing demand for greater personal data protection. Governments worldwide have responded by introducing privacy-centric policies and regulations to protect individuals' personal information. For example, the European Union's General Data Protection Regulation (GDPR) has introduced strict rules on the collection, use, and storage of personal data by companies operating in the EU.

Another reason for developing privacy-centric policies is the increasing globalization of the digital economy. With the growth of e-commerce and other online activities, personal data is often transferred across borders. Increased globalization has led to a need for international cooperation on data privacy issues to ensure that individuals' personal information is protected, regardless of where it is being processed or stored. Overall, the development of privacy-centric policies and regulations has been driven by concerns about data breaches, privacy violations, increased consumerism and the increasing globalization of the digital economy.

# Privacy Policies in different countries

Each country has unique legal, cultural, and social considerations impacting its data privacy approach. Therefore, countries have developed their policies to protect their citizens' privacy and ensure the safe and responsible use of data. These policies vary in scope and approach, but they generally aim to give individuals greater control over their data and to hold companies(data controllers) accountable for their data practices.

1. European Union (EU) - The EU has one of the most comprehensive privacy frameworks, the General Data Protection Regulation (GDPR), which came into effect on May 25, 2018. GDPR applies to all EU member states and regulates the processing of personal data of EU residents. It outlines several requirements for companies collecting and processing personal data, including obtaining explicit consent, providing access to personal data, and reporting data breaches within 72 hours. Non-compliance with GDPR can result in fines of up to 4% of a company's global revenue or €20 million, whichever is higher. (*Data Protection in the EU*, 2021)

2. United States (US)- While the US does not have a comprehensive federal privacy law, several states have passed their privacy laws, including the California Consumer Privacy Act (CCPA) and Virginia Consumer Data Protection Act (CDPA). CCPA came into effect on January 1, 2020, and requires companies to provide consumers with information about the personal data collected and allow consumers to opt out of the sale of their data. Non-compliance can result in fines of up to $7,500 per violation. CDPA, which came into effect on March 2, 2021, applies similar requirements to CCPA and has penalties of up to $7,500 per violation.

3. Japan - Japan's privacy law is the Protection of Personal Information (APPI) Act, which came into effect on May 30, 2017. APPI regulates private sector organizations' collection, use, and disclosure of personal information and requires companies to obtain explicit consent before collecting personal data. Non-compliance can result in fines of up to ¥100 million or 2% of a company's annual revenue, whichever is lower. (Usercentrics, 2023)

4. Australia: The Privacy Act 1988 governs the collection, use, and disclosure of personal information by Australian government

agencies and businesses. The act also includes the Australian Privacy Principles, which provide guidelines for handling personal information. Penalties for non-compliance can be up to AUD 2.1 million. (Usercentrics, 2023) (Oaic, 2023)

# Key takeaways for Canada

Canada can learn from the policies of these countries and their approach to data privacy. The EU's GDPR is one of the most comprehensive privacy frameworks, and Canada could consider implementing a similar law to provide more excellent protection for its citizens' data. Similarly, the US's CCPA and CDPA can serve as a model for Canadian provinces to develop their own privacy laws. Japan's APPI also emphasizes obtaining explicit consent before collecting personal data, which is a crucial principle of data privacy. Canada could consider incorporating this requirement into its privacy laws to ensure that individuals have greater control over their personal information. Australia's Privacy Act 1988 and Australian Privacy Principles provide guidelines for handling personal information by government agencies and businesses. These new E-safety platforms could serve as a model for Canadian policies to ensure that companies and organizations are held accountable for their data practices. GDPR has a solid digital rights focus, and Australia has established new platforms for individuals and businesses to define data rights. Canada can seek inspiration from the policies of these countries and their approach to data privacy to develop its own comprehensive and effective privacy laws that prioritize individual control over personal data and hold data controllers accountable for their practices.

# A deep dive into Canadian Digital Economy

# Understanding Canadian Context: Economy and Digital Penetration

## Digital Penetration

As of January 2023, Canada had over 36 million internet users, which amounted to 93.8 percent of the country's population. (Statista, 2023) It's worth noting that the COVID-19 pandemic has likely increased data consumption in Canada, as many people are working from home and using more internet-connected devices for remote work and entertainment. The vast majority of Canadians (84%) relied on a smartphone for personal use in 2020 to communicate, research, or entertainment. When asked about smartphone habits in a typical day, just over half of Canadians (53%) said that checking their smartphone was the first thing they did before waking up and the last thing they did before going to bed (51%). (Government of Canada, Statistics Canada, 2021c)

In a typical day, 43% of Canadians said they checked their smartphone at least every 30 minutes. As for younger Canadians, 71% of those 15 to 24 years of age checked their smartphone at least every 30 minutes, with 17% checking their phone every 5 minutes. (Statcan, 2020). Despite having a substantial digital penetration, Canada also has a stark digital divide with rural area internet speeds averaging 5.5 Mbps compared to 50 Mbps speeds in urban centres. (CRTC, 2022) Canada has one of the highest internet costs globally. For internet speeds of between 41 to 100 Mbps, Canada ranked third most expensive among the United States, Japan, France, Germany, Italy, the United Kingdom, and Australia.

# The Canadian Economy

Canada has a diverse economy that relies on several sectors to contribute to its GDP. The major industries that contribute to the Canadian economy include the services sector, manufacturing, natural resources, and agriculture. According to a report by Statistics Canada, the services sector is the largest contributor to the Canadian GDP, accounting for 69.1% in 2020. The manufacturing sector contributes to 10.2%, while natural resources and agriculture contribute to 7.1% and 1.6%, respectively. (Government of Canada, Statistics Canada, 2021a)

In terms of business size, Canada has a large number of small businesses, which are defined as those with fewer than 100 employees. According to a report by Innovation, Science and Economic Development Canada, small businesses accounted for 98% of all businesses in Canada in 2019. Large businesses, which are defined as those with 100 or more employees, accounted for only 0.2% of all businesses in Canada in the same year(Government of Canada, Statistics Canada, 2022a). The Canadian economy is diversified and relies on several sectors to contribute to its GDP. Small businesses play a significant role in the Canadian business landscape, while taxes collected by the government come from various sources.

The contribution of the digital economy to total gross domestic product (GDP) trended up from 5.2% ($103 billion) in 2017 to ($118 billion) in 2019. (Government of Canada, Statistics Canada, 2021) The share of the sector in overall jobs also followed a similar trend, increasing from 4.1% (772,000) of total jobs in 2017 to 4.5% (882,000) in 2019 (Government of Canada, Statistics Canada, 2021b). Canada's economy is heavily reliant on the digital sector, with technology and innovation playing a significant role in driving economic growth. The rapid expansion of the digital economy has led to the creation and processing of vast amounts of data. As a result, the importance of data privacy and data ownership has become increasingly critical in the Canadian economy.(Bank of Canada, 2021)

# Canada’s Significance - Understanding Canadian Digital Policy

Bill C-27, An Act to enact the Consumer Privacy Protection Act(CPPA), the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, is also known as the Digital Charter Implementation Act, 2022.

The Consumer Privacy Protection Act is Part 1 of the Digital Charter Implementation Act, 2022. The Consumer Privacy Protection Act would repeal parts of the Personal Information Protection and Electronic Documents Act and replace them with a new legislative regime governing the collection, use, and disclosure of personal information for commercial activity in Canada. This would maintain, modernize, and extend existing rules and impose new rules on private sector organizations for the protection of personal information.
The Consumer Privacy Protection Act would also continue and enhance the role of the Privacy Commissioner in overseeing organizations’ compliance with these measures.

Part 2 of the Digital Charter Implementation Act, 2022 contains the Personal Information and Data Protection Tribunal Act. It would create a new administrative tribunal to hear appeals of orders issued by the Privacy Commissioner and apply a new administrative monetary penalty regime created under the Consumer Privacy Protection Act.

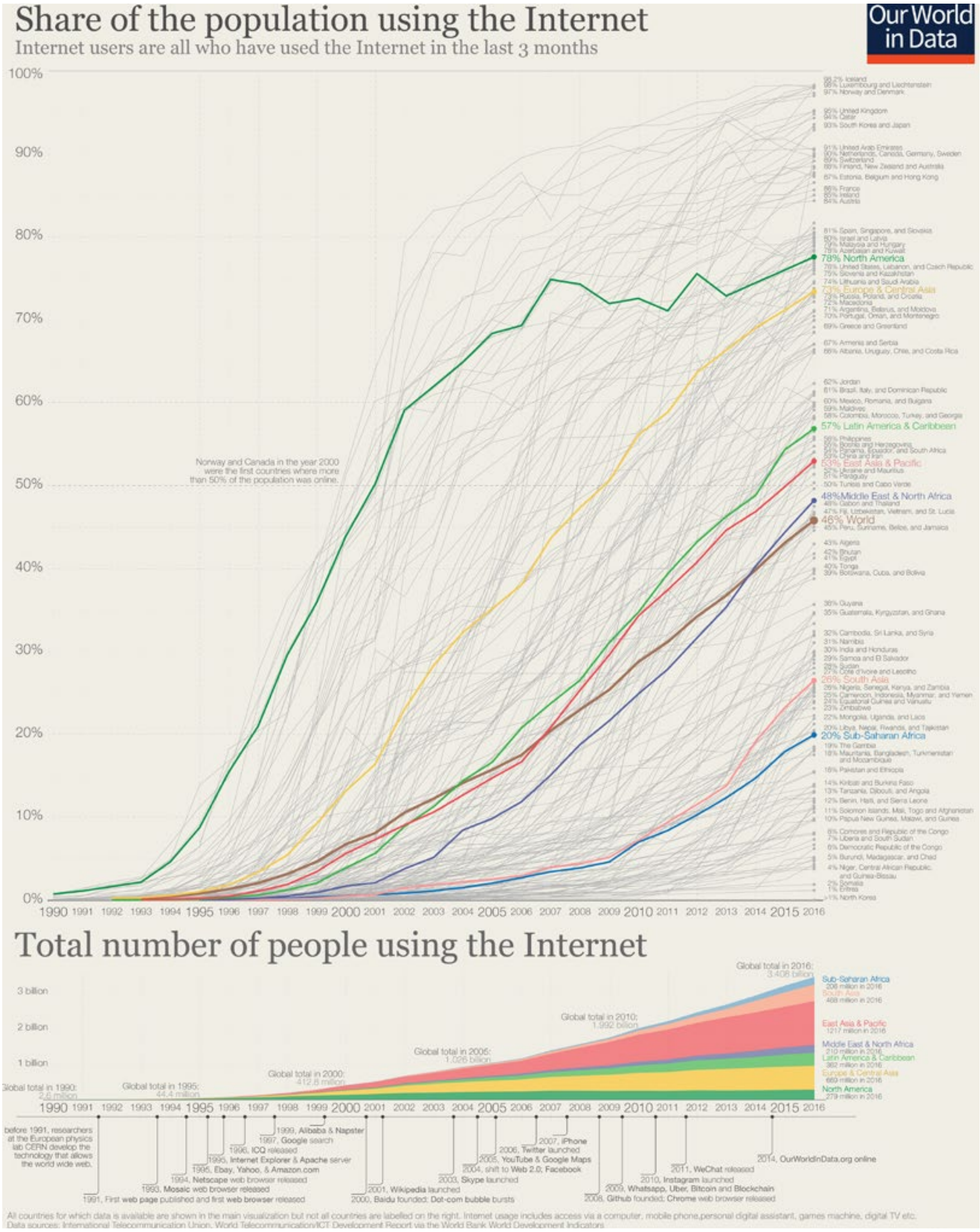
Part 3 of the Digital Charter Implementation Act, 2022, the Artificial Intelligence and Data Act, sets out new measures to regulate international and interprovincial trade and commerce in artificial intelligence systems. It would establish common requirements for the design, development, and use of artificial intelligence systems, including measures to mitigate risks of harm and biased output.
It’s worth noting that PIPEDA is currently undergoing changes, and new legislation is expected to be introduced in the near future. The proposed Digital Charter Implementation Act, 2020, includes provisions for higher fines and penalties for non-compliance with privacy laws. Under this new legislation, the maximum fine for non-compliance could be up to 5% of global revenue or $25 million CAD, whichever is higher. However, this legislation has not yet been passed and is subject to change. The introduction of fines for non-compliance will also serve as a deterrent to organizations that do not take data protection seriously. However, it remains to be seen how effective the implementation of the proposed act will be in practice.

# Key take aways from Canadian Economy and Digital Policy

The CPPA provides stronger protections for personal information, such as requiring businesses to obtain valid consent and to report data breaches to the Privacy Commissioner. The CPPA gives the Privacy Commissioner greater enforcement powers, including the ability to issue binding orders and impose fines for non-compliance. The CPPA includes new rights for individuals, such as the right to data mobility, which allows individuals to easily transfer their data from one organization to another. The CPPA is expected to provide increased accountability, improved privacy protection and enhanced consumer rights.

On the other hand, the CPPA has potential cons which includes, the CPPA does not provide adequate protection for sensitive personal information, such as biometric data or genetic information. (Gratton et al., 2023) The law only requires organizations to obtain consent for the collection, use, or disclosure of such information in limited circumstances. Additionally, there is no requirement for organizations to obtain express consent for the collection or use of personal information, which could lead to a lack of transparency and potential misuse of data. The CPPA includes provisions that require certain personal information to be stored in Canada, which may create additional compliance burdens for businesses, particularly for small businesses. Some industry participants are concerned that the CPPA may stifle innovation and limit the development of new products and services due to its stringent data protection requirements.

Another issue with the CPPA is that it places a significant burden on individuals to enforce their privacy rights, as there is no government body dedicated to privacy enforcement. (OpenMedia, 2022) Although CPPA gives digital rights to consumers, the policy is mainly directed to control big tech companies responsible for mishandling data. This means that individuals must pursue legal action on their own, which can be expensive and time-consuming. Furthermore, some critics argue that the CPPA does not go far enough in protecting the privacy of Canadians, particularly in the context of digital surveillance. (OpenMedia, 2022) For example, the law only requires organizations to provide individuals with access to their personal information upon request, rather than proactively providing individuals with detailed information about the use of their data.



# Our world in Data - Graph

The map shows the share of the population that is accessing the internet for all countries of the world. Internet users are individuals who have used the Internet (from any location). The Internet can be used via a computer, mobile phone, personal digital assistant, games machine, digital TV etc.

Norway and Canada were the first countries in 2020 to where more than 50% of the population was online. Currently, 97% of the population in Canada has onboarded on the digital bandwagon. In turn, rising a demand in consumerism, data privacy, digital rights and ethical data practices across all online services and mediums.

# What is on the horizon?

# Emerging shifts on the horizons

We must assess where we currently stand to comprehend the direction we are moving towards. A trend scan is a valuable tool for analyzing emerging innovations and attitudes and creating a comprehensive framework for evaluation. By observing the developing advancements in our global landscape, we can uncover the underlying trends driving these changes. By comprehending these shifts, we can anticipate their long-term implications.

In the following pages, the research will come across various emerging shifts and its implication reflecting the changing beliefs and behaviours of our technological, economic, and societal systems. Although this list is not exhaustive, it represents a broad examination of the evolving attitudes of our society. Notably, many of these trends are separate from data policies, as understanding our societal values at a broader level is essential in determining their impact on specific behaviours and sectors. The breadth of emerging shifts demonstrates the importance of exploring how the external systems that guide and govern data could drive future change. Possible implications and related trends of the emerging potentialities are shown below

# Shift Towards Privacy-Centric Future Gains Momentum

# Shift Towards Privacy-Centric Future Gains Momentum

## Description

The increasing consumer concern regarding data privacy is a response to the growing awareness of the risks associated with the widespread collection and use of personal information. Consumers are becoming more aware of the ways in which their data is being collected, stored, and used, and they want to have more control over their personal information. This has resulted in a higher tendency to avoid businesses that do not prioritise data privacy. Consumers are demanding more transparency and protection of their individual rights, and they are taking proactive steps to safeguard their data privacy. The study did find that 71% of respondents took the time check their advanced privacy settings when they joined a social media platform(Suciu, 2020) However, the sheer amount of personal data collected online presents a significant challenge to these efforts. Many consumers are aware of the risks associated with sharing their personal information, but they may not have a clear understanding of how their data is being used or who has access to it(Auxier et al., 2020). This highlights the need for more comprehensive data privacy policies and practices that give consumers greater control over their personal information.

As a result of these concerns, there has been a gradual rise in the adoption of privacy-protected services. Consumers are seeking out services that prioritize data privacy and security, and they are willing to pay more for these services(Mckinsey & Co, 2020). This trend is likely to continue as consumers become more informed about the risks associated with sharing their personal information online and demand greater transparency and protection of their data privacy rights.

## Related trends

1. Decline in Public Trust: as personal data is repeatedly shown to be insecure and used for unintended or nefarious purposes, trust in digital systems is eroded, regardless of whether maintained by public or private institutions.

2. The GDPR standards: The GDPR sets a new standard for data protection, putting individuals in control of their personal data and imposing strict rules on how organizations collect, process, and store data. This is a significant shift from the previous model, which placed the burden of protecting personal data on individuals

# Implications

1. Canadian economy: As consumers become more concerned about their data privacy, businesses that prioritize privacy protection will have a competitive advantage. This could result in a shift towards a more privacy-centric Canadian economy, where businesses that respect individuals' privacy rights are more successful.

2. Canadian culture: Privacy is an important value in Canadian culture, and the shift towards a privacy-centric future could further increase. Canadians may begin to expect greater privacy protections from businesses and governments, and there may be a greater emphasis on individual privacy and digital rights.

3. Canadian digital economy: The digital economy in Canada may become more privacy-focused, with businesses and consumers alike demanding better protection for personal data. This could lead to the development of more privacy-centric technology solutions and services in Canada, which could help to strengthen the country's position as a leader in the digital economy.

4. Privacy-Centric Innovations: New encryption methods such as homomorphic encryption and pseudonymization could change how data is processed, analyzed, and used. This may increase the reliance on synthetic datasets. The shift towards a privacy-centric future may have both positive and negative implications for innovation and interoperability.

5. Biometric data collection: With the rise of biometric data collection, policy makers will need to ensure that there are clear regulations and guidelines in place to protect individuals' privacy rights. The collection, storage, and use of biometric data must be done in a transparent and ethical manner, with individuals' informed consent.

6. Changes in business model: Small businesses may struggle to keep up with the changing landscape of data privacy. They may lack the resources or expertise to implement strong privacy protections, which could put them at a disadvantage compared to larger businesses. As small businesses are the back bone of Canadian economy, policy makers may need to consider providing resources and support to small businesses to help them adapt to the new privacy-centric environment

7. Digital divide: Canada has a huge digital divide in remote or rural areas where access to high-speed internet and digital technologies can be limited. This can result in unequal access to information, education, and job opportunities. The could have positive as well negative effects on the economy. The government needs to  implement various initiatives to improve digital infrastructure and accessibility in under-served areas.

## Signals

1. VPNs, or virtual private networks, have become indispensable tools in today's internet-driven world and internet-fed culture. The market for VPNs has been growing at an increased pace since the COVID-19 pandemic, and it's expected to surpass $92 billion in 2027.

2. A meta-analysis published published on Wiley Online Library with total of 166 studies from 34 countries shows that as privacy literacy increases the users were less likely to online services and share information and were more likely to utilize privacy protective measures.

3. According to Mckinsey research only about one third of population believe that companies are using their personal data responsibly. Two-thirds of the population have neutral to negative view.

4. Ghostery for Android or iOS installed, and straight away it gets to work blocking adverts and tracking cookies that will attempt to keep tabs on what you're up to on the web.

5. Brave is a project from Brendan Eich, once of Firefox developer Mozilla, and its mission includes both keeping you from being tracked on the web, and finding a better way to serve you advertisements.

6. Apple continues to pile privacy-focused features into its Safari browser, and people are more aware than ever before of the sort of information they can reveal every time they set a digital footprint on the web.

7. An Israeli startup called 'Mine', that protects locates and calculates the risk of your data and deletes users data by sending an automated email request from the user's own account. Mine has successfully raised 9.5 million.

# Technology: The next arms race

# Technology: The next arms race

## Description

Technology has become a key factor in determining the geopolitical power balance, with nations and corporations alike striving to stay ahead of the competition in developing cutting-edge technology. The proliferation of advanced technologies such as artificial intelligence, autonomous systems, and cybersecurity has created a new kind of arms race, where nations are vying to develop the most advanced and capable technologies. This competition is driven by the recognition that technological superiority can provide a significant strategic advantage in a variety of domains, including military, economic, and political(Hirsh, 2023). For instance, militaries around the world are increasingly investing in advanced technologies like drones, cyber weapons, and AI-powered autonomous weapons systems to gain a competitive edge on the battlefield.

Dozens of countries are exploring military uses of AI. Most research and development happens within the private sector and, critically, many of the most exciting breakthroughs are “dual use” — they have civilian and military applications. (Brands, 2023) At the same time, the growing amount of personal data being collected by governments and companies raises concerns about privacy violations and surveillance. As individuals’ personal information becomes more accessible and potentially vulnerable, there is a risk of identity theft, financial fraud, and other forms of privacy violations. In some cases, governments may also use data collection and surveillance to monitor citizens’ activities and suppress dissent. As the use of technology becomes more ubiquitous, individuals may find it increasingly difficult to maintain control over their personal information.

## Related trends

1. New Currencies: Data is now a recognized commodity, in a way that it has not been appreciated before, which means that we are beginning to see a prescribed valuation emerge.

2. An echo chamber is an environment where a person only encounters information or opinions that reflect and reinforce their own. Echo chambers can create misinformation and distort a person’s perspective so they have difficulty considering opposing viewpoints and discussing complicated topics. They’re fueled in part by confirmation bias.

# Implications

1. Economic impact: The technology arms race can have a significant impact on the Canadian economy, as companies and industries that do not keep up with technological advancements may struggle to remain competitive and might be prone to cyber-attacks. Policymakers must identify and support emerging industries that have the potential for growth and job creation.

2. National security: Traditional forms of warfare may become less effective as countries increasingly rely on cyber attacks and other forms of technology-based aggression. Counter-surveillance technologies must be developed to protect government data and infrastructure. As data flows across borders, policy makers need to consider international agreements and frameworks, such as the Canada-United States-Mexico Agreement (CUSMA), to ensure privacy protection for Canadians' personal information.

3. Canadian Culture: Policymakers will need to consider the potential impact of technological advancements on social structures, cultural norms, and values. As the use of advanced technologies such as autonomous systems and artificial intelligence become more widespread, there may be concerns around the impact on human autonomy and decision-making.

4. Data breach: Policymakers should should enforce strong frameworks and guidelines for businesses to ensure that personal information is protected and individuals are notified promptly in the event of a breach. A regulatory body can be created which audits or issues compliance proofs towards safe and secure data networks.

5. Technological Pace: As the technological pace increases, there will be continued growth and investment in areas such as artificial intelligence, quantum computing, and 5G networks. Conversely, older technologies that are less secure and less capable, such as legacy IT systems and older communication networks, may become obsolete as they are replaced by newer, more advanced technologies.

6. Canadian digital economy, policymakers will need to ensure that the country remains competitive in the development and deployment of advanced technologies. This may involve supporting the growth of domestic tech companies, incentivising foreign investment, and fostering a supportive regulatory environment.

# Signals

1. Russia supplies Iran with cyber weapons in exchange for drones and ammunition. Russia has supplied Iran with surveillance and intelligence gathering equipment, hidden cameras, and lie detectors.

2. China has long used Taiwan as a testing ground for its cyber capabilities. China attacked convenience store, high-speed rail station, Hackers even brought down Taiwanese president Tsai Ing-wen's official government website for around 20 minutes.

3. In 2019, LifeLabs, a medical laboratory services company, reported that it had suffered a data breach that affected the personal information of approximately 15 million Canadians. The breach included information such as names, addresses, birth dates, and lab test results. The company later paid a ransom to the hackers in exchange for the stolen data.

4. Hackers working on behalf of China were stealing thousands of emails and sensitive details from the Southeast Asian nations. Chinese-linked hackers were able to break into mail servers operated by the Association of Southeast Asian Nations (ASEAN) in February 2022 and steal a trove of data

5. Pegasus is the hacking software – or spyware – that is developed, marketed and licensed to governments around the world by the Israeli company NSO Group. Once it has wormed its way on to your phone, without you noticing, it can turn it into a 24-hour surveillance device.

6. The WannaCry ransomware attack affected hundreds of thousands of computers in more than 150 countries, causing widespread disruption and financial losses in 2017.

7. In 2018, the United States accused Russia of conducting a cyberattack on the Ukrainian power grid, which caused widespread power outages and disruption.

8. Financial data of over 9M cardholders leaked from an Indian government bank SBI. The hackers released sensitive Personal Identifiable Information (PII) information such as SSN, card details and CVV

9. Intel, I.B.M., Microsoft, and Amazon are also building quantum computers. So is the Chinese government. The winner of the race will produce the successor to the silicon microchip, the device that enabled the information revolution. A full-scale quantum computer could crack our current encryption protocols, essentially breaking the Internet.

# Age of Surveillance: A new normal

# Age of Surveillance: A new Normal

## Description

The increasing use of surveillance technologies and practices in our daily lives has marked the Age of Surveillance. Surveillance capitalism describes a market-driven process where the commodity for sale is csonumers personal data. The capture and production of this data rely on mass surveillance of the internet. This activity is often carried out by companies that provide us with free online services, such as search engines (Google) and social media platforms (Facebook)(Holloway, 2019). The rise of digital technologies has resulted in a vast amount of data being generated, which can be used to monitor and track our activities. Several types of surveillance have emerged, including physical surveillance, which involves the use of cameras and drones, digital surveillance that tracks browsing history and social media posts. Biometric surveillance uses facial recognition and fingerprinting, social surveillance that monitors behaviour and interests, and luxury surveillance, which is traded for benefits such as security or convenience.

The implications of the Age of Surveillance are complex and far-reaching. On the one hand, surveillance technologies can be used to improve public safety and security by monitoring potential threats and preventing crime. They can also enhance business operations and provide personalized services to consumers. However, these technologies can also be used to violate privacy and monitor dissent, leading to concerns about government overreach and the potential for abuse.

## Related trends

1. New Currencies: Data is now a recognized commodity, in a way that it has not been appreciated before, which means that we are beginning to see a prescribed valuation emerge.

2. The rise of Big Data Policing: Big data policing refers to the use of sophisticated data analytics tools and techniques to analyze large amounts of data generated by various sources to identify criminal activities and prevent crimes.

# Implications

1. Interest in decentralised technologies: Decentralised technologies such as blockchain and peer-to-peer networks may gain more interest as people seek to regain control over their personal data and activities.

2. Increased marginalisation: Real-time data collection technologies might be able to track societal lawfulness in real time. This could reduce criminal activity within urbanised areas. However, it could reinforce biased algorithms negatively impacting marginalised populations. Policy makers need to consider the harms and history of Canada as well.

3. Counter-surveillance technologies, devices that allow you to be undetected, could become commonplace. A counter culture might emerge of urban residents moving to remote self-sustaining communities without technology. This could create new complications for the census in tracking population movements, increased suspicion and mistrust among individuals and communities.

4. The development and dissemination of counter-surveillance technologies may exacerbate existing power imbalances between those who have access to these technologies and those who do not, potentially leading to new forms of surveillance and control.

5. Trust in centralised institutions: As surveillance becomes more prevalent, there may be a decline in trust towards centralised institutions such as governments and corporations. Data black markets could emerge consisting of personal data attained in unlawful ways. These databases could diminish trust in centralised institutions.

6. Ethics and Human Rights: As surveillance grows, policymakers need to ensure that surveillance technologies are not used to infringe upon human rights, such as freedom of expression and association, and that they are used in a manner that is consistent with ethical standards.

7. Unequal distribution: Surveillance technologies are not equally accessible or affordable to everyone, which can lead to an unequal distribution of power and access to information.

8. Increased Efficiency: There could be increased investment

in digital government services. This could include AI assistants to guide user experiences through government services and portals. Surveillance technologies can also help emergency responders quickly identify and respond to emergencies, potentially saving lives.

## Signals

1. China has a huge breadth of data collection. The Chinese government has access to probably about 400 million cameras across the country. Beyond access to those 400 million cameras, the Chinese government still has access to about a billion smartphones that the Chinese citizens use

2. According to 2021 research by CCTV.co.uk, the total number of CCTV cameras in London is 691,000, or roughly 1 for every 13 people.

3. The capital city of India, Delhi has 436,600 cameras for every 16,349,831 people that is 26.7 cameras per 1000 people

4. Amazon already has a reputation for turning low-paid staff into “human robots” Amazon has patented designs for a wristband that can precisely track where warehouse employees are placing their hands and use vibrations to nudge them in a different direction.

5. Both the Apple Watch and the FitBit can be understood as examples of *luxury surveillance*: surveillance that people pay for and whose tracking, monitoring, and quantification features are understood by the user as benefits they are likely to celebrate.

6. The NYPD’s Social Media Unit monitors social media platforms to identify potential threats to public safety and investigate crimes.

7. Social Intelligence, a company located in Santa Barbara, California, they specialise in social media monitoring and background screening for potential job candidates, so the company is alerted to potential problems or issues that might be considered contentious.

8. The Ring doorbell company, owned by Amazon, has partnered with more than 400 law enforcement agencies in the US, allowing them to request footage from the company’s cameras. Users, which the company calls “neighbours,” are anonymous on the app, but the public video does not obscure faces or voices from anyone caught on camera.

# Responsible and Ethical Tech on the Rise

# Responsible and Ethical Tech on the Rise

## Description

In the past year, tech worker mobilization has reached unprecedented levels. Kickstarter employees sought union recognition from their company. Amazon workers led a cross tech-industry walkout to support the global climate strike. Googlers grappled with unionization, fought against increasing corporate hostility, and challenged their company's unethical partnerships.(Reporter, 2020) Many individuals within the technology industry are starting to question the direction in which technology is headed, as they see the potential for negative consequences. This has resulted in a growing number of tech activists, non-governmental organizations, and independent tech journalists who are advocating for more ethical and humane use of technology. Tech skeptics are challenging the current paradigm and are working towards developing structures, frameworks, and systems that promote equitable and more humane practices. There are already many students and young professionals readily willing to pursue a career in public interest tech, and plenty of research institutes and academic programs building a bank of knowledge for the sector. (Irwin, 2022) They call it public interest technology. Public interest technologists seek to center the perspectives of historically marginalized groups—including Black, Indigenous and people of color, women and the disability community—because they are most harmed by technology but also have the knowledge and experience to ensure technology advances justice. (Public Interest Technology and Its Origins, 2022)

The concerns raised by tech skeptics include issues such as data privacy, the impact of automation on employment, the potential for algorithmic bias, and the proliferation of misinformation online. These issues have far-reaching consequences, including the potential for the erosion of democracy and human rights.

## Related trends

Tech Addiction:With technology constantly feeding us content that aligns with our beliefs, it's comforting to be surrounded by familiar and unchallenging narratives in this age of uncertainty.

People opting for privacy centric services:With increasing concerns around data privacy and security, more and more people are opting for privacy-centric services that offer greater control and protection over their personal information.

# Implications

1. Changes in business models: As more stringent privacy regulations are implemented, businesses that rely heavily on collecting and using consumer data may need to adjust their business models. This could lead to disruptions in industries such as advertising and e-commerce

2. New opportunities: There will likely be a high demand for privacy, ethics, and compliance managers. These professionals will be responsible for ensuring that companies and organizations are following the relevant data privacy laws and regulations, implementing ethical data practices, and protecting individuals' privacy rights.

3. Strengthening Locals: Governments and policy makers can strengthen ethical data practices at a grass root level which is Municipalities. Often Municipal governments are under funded and do not have the means to execute local concerns. An infrastructure or a data ecosystem can be built by considering the local government needs.

4. A rise in consumer activism: As consumers become more aware of the implications of their data privacy, they may become more vocal about their concerns, advocating for stronger regulations and demanding more transparency from companies. This could also rise in e-NGOs which provide education, knowledge awareness about data ethics and use.

5. Formation of new bodies: Government and businesses need to be aware of the regulatory environment and ensure that they are compliant with privacy laws. The role of compliance managers, ethicists and privacy officer will become ubiquitous, hence policy makers and businesses need to invest in relevant technologies and infrastructure.

6. Shift in consumerism: Consumers making more informed purchasing decisions and supporting businesses that prioritize social and environmental responsibility. It can also lead to a shift away from traditional consumerism and towards a more mindful and conscious approach to consumption.

7. Shift towards value based work: Employees in the tech organization are leaving due to ethical considerations of data, this may lead to a shared value work culture where employee work with companies which prioritise privacy, data ethics and environmental

responsibility

8. New initiatives could emerge for the interoperability of private and public sector databases. The connections between databases could become integrated in efforts to govern the technology sector.

## Signals

1. Founded in 2018. All Tech Is Human is a non-profit organisation that has intentionally brought together a diverse range of individuals and organisations across civil society, government, and industry. All Tech Is Human curates roles focused on reducing the harms of technology, diversifying the tech pipeline, and ensuring that technology is aligned with the public interest.

2. The Algorithmic Justice League(AGL), an NGO, is an organisation that combines art and research to illuminate the social implications and harms of artificial intelligence. AGL works towards gender and racial disparities in algorithms and AI systems.

3. RadicalxChange (RxC) is a global movement for next-generation political economies. They are committed to advancing plurality, equality, community, and decentralization through upgrading democracy, markets, the data economy, the commons, and identity. They have proposed concepts like plural voting, plural funding, plural property and data dignity.

4. Center for Humane Technology(CHT) claims credit for inducing numerous social media and technology companies to introduce user interface changes designed to limit the harms of their use. Additionally, CHT has created toolkits for policy makers, kids, and adults to take control from technologies.

5. New_ Public is a place for thinkers, builders, designers, and technologists to meet, share inspiration, and make better digital public spaces. It's a newsletter, magazine, and community wrapped together, supported by the team at Civic Signals.

6. EY identified that only 42% of this segment say they are satisfied with their quality of life at present, and 54% feel that the world is changing too fast.

7. Tactical Tech, a Berlin-based non-profit organisation, engages with citizens and civil-society organisations to explore and mitigate the impacts of technology on society.

# Corporatocracy: Rising Influence of Big Tech

# Corporatocracy: Rising Influence of Big Tech

## Description

The growing influence of corporations and big tech in politics and governance has raised concerns about the integrity of democratic institutions worldwide (Anderson et al., 2022). With vast resources at their disposal, corporations are able to wield significant power and influence over governments and public policy. This includes the ability to sway election outcomes through targeted advertising and social media campaigns and censor or amplify specific messages to shape public opinion. (Naughton, 2021) In addition, the concentration of wealth and power in the hands of a few large corporations has led to concerns about the potential for privatized statehood, in which corporations effectively control government functions. (IMF, 2018) The influence of tech companies could lead to a situation in which government policy is driven not by citizens' needs and interests but by corporate entities' profit motives.

These developments threaten to redefine the very nature of democracy, raising questions about the role of corporations in public life and the ability of citizens to hold their elected representatives accountable. (Anderson et al., 2022) As a result, many governments worldwide are calling for increased regulation of corporate influence in politics and the establishment of safeguards to protect the integrity of democratic institutions.

## Related trends

Digital decentralization:Alternate technology systems are rising which are distribution of power and control over digital systems and data, away from centralized entities and towards individuals or smaller, decentralized networks.

Regulation of big tech: With big tech becoming more powerful, legal frameworks and policies put in place by governments to control the behavior of big technology companies and to protect consumers from potential harms such as privacy violations, anti-competitive practices, and manipulation of information.

# Implications

1. In terms of Canadian culture, there may be concerns about the impact of foreign influence on Canadian media and politics. The government may need to take steps to protect Canadian media from foreign interference, as well as to promote media literacy and critical thinking skills among citizens.

2. For businesses, there may be increased pressure to adhere to regulations and guidelines regarding political influence and advertising. Companies may need to be more transparent about their political donations and lobbying activities. There may also be a shift towards supporting companies that prioritize ethical business practices and are more transparent about their political activities.

3. With rise of big tech, policy makers may consider measures to protect Canadian businesses from being bought out by big tech companies, such as stricter foreign investment rules or incentives for Canadian companies to remain independent.

4. There may also be a need for increased investment in Canadian digital infrastructure to ensure that Canadian businesses are not overly reliant on big tech companies for their technology needs. This could include investments in high-speed internet access, cybersecurity, and digital innovation.

5. Corporations may exacerbate inequality by prioritizing the interests of their shareholders over those of their employees or other stakeholders, which can lead to disparities in wealth and opportunity in Canada.

6. Most of the tech giants like Google and Facebook are headquartered in the United States, which means they are primarily subject to U.S. laws. The storage of Canadian data lies in the hands of US enforcement agencies and personnel. Data breach or cyber-war in US could affect privacy and security of Canadians leading to a strong change in US-Canada bi-lateral relations

7. Governments could create new taxation models treating the harvesting of personal

data by the private sector as labour. This new model would likely be unsustainable for big tech companies leading them to stop selling user data, declare bankruptcy or charge huge fees to individual user leading to unaffordable technology costs.

# Signals

1. Google and Big Tech can shift millions of votes in any direction — Tech companies using algorithms to push favouritism, amplify biased political messages and influence opinions of the masses.

2. Addressing Big Tech's power over speech — At many points during the 2020 U.S. presidential election, social media platforms demonstrated their power over speech. Twitter decided to ban political advertisements permanently in October 2019, sparking a vigorous debate over free speech and so-called "paid disinformation (Chin, 2021).

3. Apple, Amazon Wealthier than More than 90% of the World's Countries — In 2018, Apple became the first company to surpass the trillion-dollar value mark — and has more than doubled its value since. Now worth a cool $2.2 trillion, compared to the wealth of countries' worldwide — it would be the 8th richest country in the world

4. In the UK, Big Techs were invited to Downing Street to discuss the tech solutions required to overcome Covid-19, which saw the surveillance giant Palantir earn lucrative contracts to streamline data flows across the state.

5. In October 2020, Apple, Microsoft, Amazon, and Alphabet had each crossed the threshold of a $1 trillion market capitalisation.

6. At a market cap of more than $2.1 trillion, Apple's market capitalization is larger than 96% of country GDPs, a list that includes Italy, Brazil, Canada, and Russia.

7. The security services of major democracies are using Amazon Web Services (AWS). Just to take a couple of examples, the CIA has been using it since 2014 and recently it was revealed that the UK's spy agencies have given a £500m-plus contract to AWS to host classified material to boost the use of data analytics and "AI"

8. An intrepid journalist named Kashmir Hill conducted an interesting experiment to cut her access from all tech giants. The results of Ms Kashmir's experiment revealed that our lives now run on a technical infrastructure that is owned, operated and controlled by a handful of giant corporations, from which there is currently no escape unless you plan to hibernate.

# Considerations for scenario development

Several insights emerged through the process of developing the emerging shifts. The insights from this section are summarised below:

1. With rise of digital ecosystems and digital services, the consumerism culture is subjected to increase leading a greater need for privacy officers and enforcement agencies that address privacy concerns.

2. Tech activists and privacy-centric consumer activists recognise the harms of technology and complex nature of data sharing ecosystems. Regulating or changing the ecosystems requires stakeholder collaboration. Stakeholders outside of the Government are becoming more willing to enact change when there is an economic incentive.

3. The CPPA holds all data collecting organizations with high standards, since 98% of Canadian businesses are small businesses, this might raise concerns that the compliance costs associated with the new regulations may be disproportionately burdensome for small businesses with limited resources.

4. Under the CPPA, it can be challenging for organizations to identify all personal information that may be considered sensitive due to the lack of clear definition and the need to consider various contextual factors. While some categories of personal information are almost always considered sensitive, others may only be sensitive in certain situations. Compliance with this requirement may vary greatly among organizations as it may not always be apparent whether the information held is sensitive under the CPPA.

5. Governments and multilateral organizations are pursuing efforts to regulate AI and facial recognition technologies. However, it is uncertain whether these technologies can be controlled given the speed of technological innovation and ubiquity of data collection technologies.

6. In the world of cyber-war and data breaches, it paramount to create technological superiority on Canada's soil to protect digital infrastructure from any intrusions, data breaches and privacy violations. Investments in encryptions, quantum computing and autonomous systems are crucial.

The analysis of the emerging shifts demonstrates that there are several areas of critical uncertainty that could change in different directions. These uncertainties will be explored in the future scenarios. The scenarios will demonstrate the possible futures related to data ecosystem and carve out recommendations for effective data policies.

# The Future: What are the possibilities?

What is likely to emerge?

What do we want and what do we want to avoid?

What are the lessons learnt from foresight?

# The Current Paradigm

Sohail Inayatullah's (2008) CLA is used to describe why the system works in its current state. The analysis starts from the visible layers of the system (litany) and then moves downwards describing the deeper systemic underpinnings.

The definitions of each layer are outlined below:

**Litany (continuous): What is visible today within the system boundaries.**

**Systemic manifestations (years): historical explanations for the visible activities.**

**Worldview (decades): the underlying beliefs guiding the system.**

**Myth/Metaphor (societal/civilizational): a headline describing system actors' perceptions of the three layers above.**

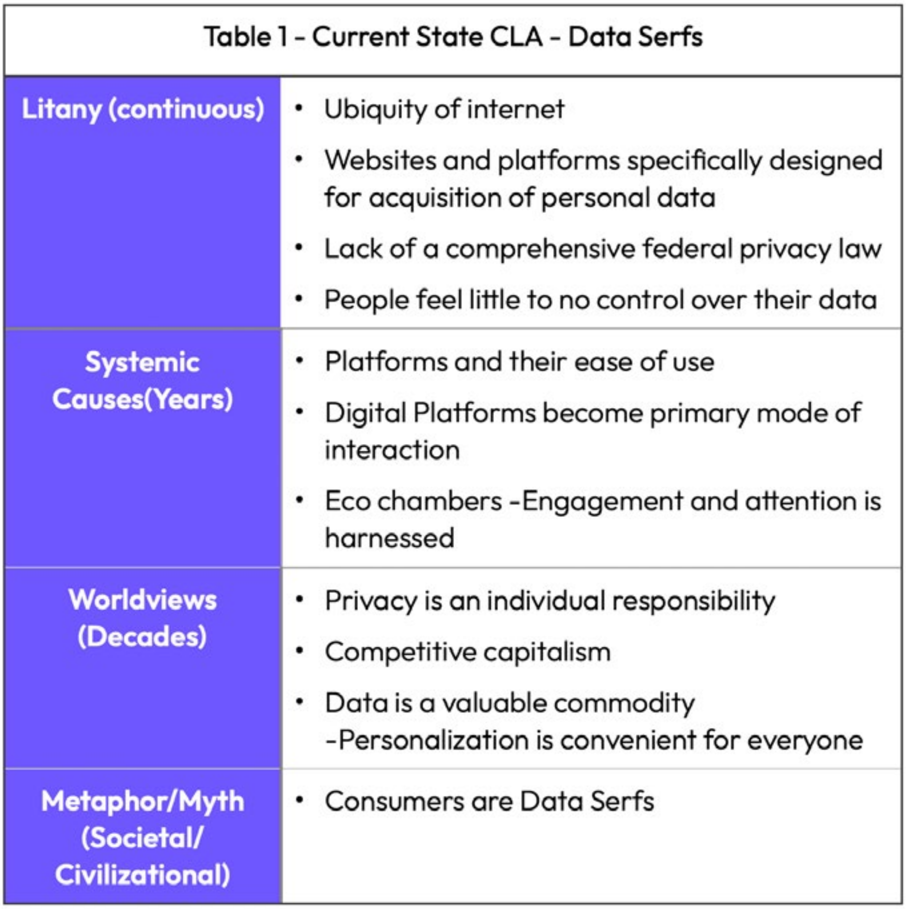


Table 1 - Current State CLA - Data Serfs

| | |
|---|---|
| Litany (continuous) | • Ubiquity of internet<br>• Websites and platforms specifically designed for acquisition of personal data<br>• Lack of a comprehensive federal privacy law<br>• People feel little to no control over their data |
| Systemic Causes(Years) | • Platforms and their ease of use<br>• Digital Platforms become primary mode of interaction<br>• Eco chambers -Engagement and attention is harnessed |
| Worldviews (Decades) | • Privacy is an individual responsibility<br>• Competitive capitalism<br>• Data is a valuable commodity<br>-Personalization is convenient for everyone |
| Metaphor/Myth (Societal/ Civilizational) | • Consumers are Data Serfs |

# Analysis of Current State

## Litany(continuous)

- **Ubiquity of Internet**

- **Digital platforms specifically designed for acquisition of personal data**

- **Lack of a comprehensive federal privacy law**

- **People feel little to no control over their data**

Modern companies worldwide introduce technology-based innovations not only to streamline their business operations and increase competitive advantage – but also to carve out new markets (Wang and Xu, 2018) The ubiquity of the internet and the emergence of websites and platforms specifically designed for the acquisition of personal data have created a situation where individuals' data is constantly being collected and used in ways they may not fully understand. In Canada, there is a lack of a comprehensive federal privacy law, leaving citizens vulnerable to the exploitation of their personal information. The resulting lack of control over their data has led to frustration, mistrust, and even helplessness among individuals. Moreover, the rise of surveillance capitalism has led to companies monetizing personal data, leading to further concerns about privacy and data ownership. The rise of platforms is concurrent with the evolution of the digital economy, with both public, private and individual networks seeking the benefits of technology that have now been ingrained into everyday life (Murphy, 2017). For example, Google and Facebook are known to generate revenue through targeted advertising using users' data.

Eventually, this data gets synthesized into a valuable product or service offering to be used by consumers. This reinforcing system satisfies the platforms' demand for a continuous supply of their most important asset. (United Nations, 2019).

# Systemic Causes (Years)

- **Platforms and their ease of use - usability and internet user experience draw people in**
- **Eco chambers**
- **Engagement and attention is harnessed**

By the 2000s, so much information was being generated worldwide that only a small fraction (0.5% in 2015) of the digital data generated was being analyzed at all. This made information relatively cheap, while the “price of attention” has risen much faster since the advent of the internet in the 1990s. Due to the scarcity of people’s attention, these technologies are increasingly aimed at strategically capturing personal attention aided by systematic collection and analysis of personal data, which has become a very profitable business model. The ease of use and intuitive nature of social media platforms and websites have made them highly appealing to Internet users, contributing to their widespread use. (Goldhaber, 1997) Platforms’ ability to provide personalized content based on user data creates echo chambers where users are often exposed to only one perspective or ideology, further polarizing society and limiting the diversity of information received. It’s been found that only about 4 percent of people operate in online echo chambers, and most people are on Twitter(Benson, 2023). The use of engagement and attention algorithms by platforms also contributes to the addictive nature of these services and the constant need for users to consume more content. The need for more transparency in how the platforms operate since the conception of the digital economy has resulted in inadequate governance of platform companies (Chew et al., 2018). These systemic causes contribute to the rapid spread of misinformation and the difficulty of breaking out of one’s echo chamber, further exacerbating the lack of control individuals have over their data and its use. The echo chamber may be comforting, but ultimately it locks us into perpetual tribalism and does tangible damage to our understanding, leading toward cyberbalkanization(Grimes, 2018)

# Worldviews (Decades)

- **Privacy is an individual responsibility**
- **Competitive capitalism**
- **Data is a valuable commodity**
- **Personalization is convenient for everyone**

The rise of big tech within the platform economy has embraced a ‘data as an asset’ business model. This model has become core to the data economy and underpins a complex ecosystem of tech companies, data brokers, advertisers and beyond. (Amnesty International, 2021) Additionally, the dominance of competitive capitalism has led to prioritizing profits over protecting personal information. The perception that data is a valuable commodity has resulted in the exploitation of personal information by businesses and organizations for financial gain. Social media platforms are seductive, and people may experience pressure to join them as they feel they are missing out on not using them or may be forced by an employer to join them. (Nycyk, 2020) The primary cultural worldview in this layer is the nonchalant attitude of internet users that privacy no longer exists in the online and outer world. Hence, it is the consumer’s responsibility. This worldview supports the desires of internet users for privacy and outrage when this is broken, which is often expressed in data breaches like Ashley Madison’s dating name and email address hacking incident or Cambridge Analytica. Companies may collect and use personal data without providing clear information to individuals about how their data is being used or who it is being shared with (Nycyk, 2020). This lack of transparency can lead to a lack of accountability and trust between companies and individuals.

# Metaphor/Myth (Societal/Civilizational)

- **Cosumers are Data Serfs**

Big tech platforms have succeeded in operating in monopolies over their existence, contributing to the cannibalization of many organizations that sought to compete in the same markets. (Naughton, 2019a) The Internet of Things is less about convenience than it is about commerce. Not only do companies sell us the gadget, but we continue to pay rent to the company by giving them our data, which they can mine to sell us more things, or sell the data itself to another company that wishes to sell us more things. Feudalism says that power rests with those who control the means of production. In the middle ages, that meant the kings and nobility who owned the land. In the industrial revolution, it meant the people who owned the factories and eventually the governments who controlled and regulated them. (Marr, 2016) Access to the internet becomes affordable and more widespread worldwide. Therefore, as beliefs influence behaviours that create new cultures (or even create new realities), internet users have come to expect tradeoffs with their data that are much like the lord and peasant relationship in medieval times.  The technological companies may take it for granted that internet users are willing serfs and that companies and governments can mine their data and profile their customers for any number of reasons. (Nycyk, 2020) Just as feudal serfs in the middle ages could never advance to the point of owning the land they worked, because the deck was stacked against them, so consumers could never escape the automation and technology we lease from the digital overlords.(Marr, 2016)  Currently we are seeing the reflections of it. For eg: The latest gadget, you must agree to the company’s terms. If consumers opt out, consumers cannot use their technology.

**“The influence of modern physics goes beyond technology. It extends to the realm of thought and culture where it has led to a deep revision in man’s conception of the universe and his relation to it”**

**- Fritjof Capra**

# Moving from present to future

The future state CLA is built from the current state CLA. The current state CLA's myth/metaphor was contextually flipped to create an alternative myth/ metaphor that would be more conducive to a desired alternative future scenario. This process starts from the myth, which will help to inform new characteristics of the worldview, systems and litany. Starting from the deepest layer of the system creates an opportunity to work at changing the goal and root cause of the issues at hand.

Figure: This figure demonstrates how Inayatullah's (2008) CLA is used in problem framing. The alternative CLA begins with three alternative metaphors that challenge the current state metaphor.

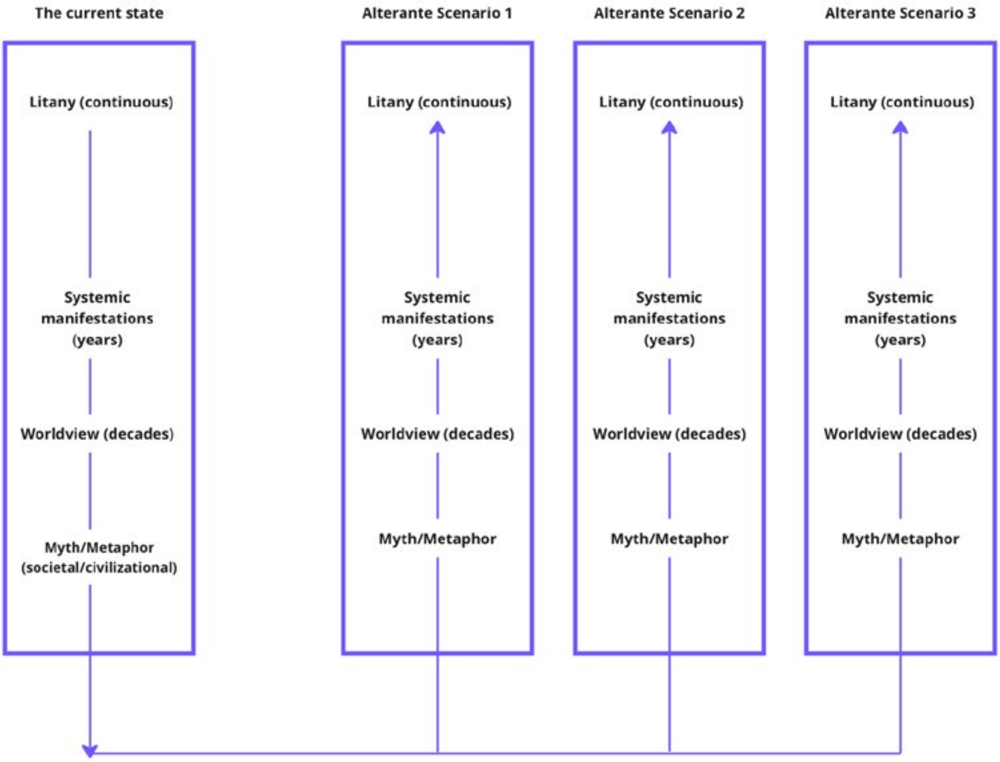


Figure 1 : Moving from present to future shows the path of creating alternate scenarios with different myths and metaphors to imagine new worlds

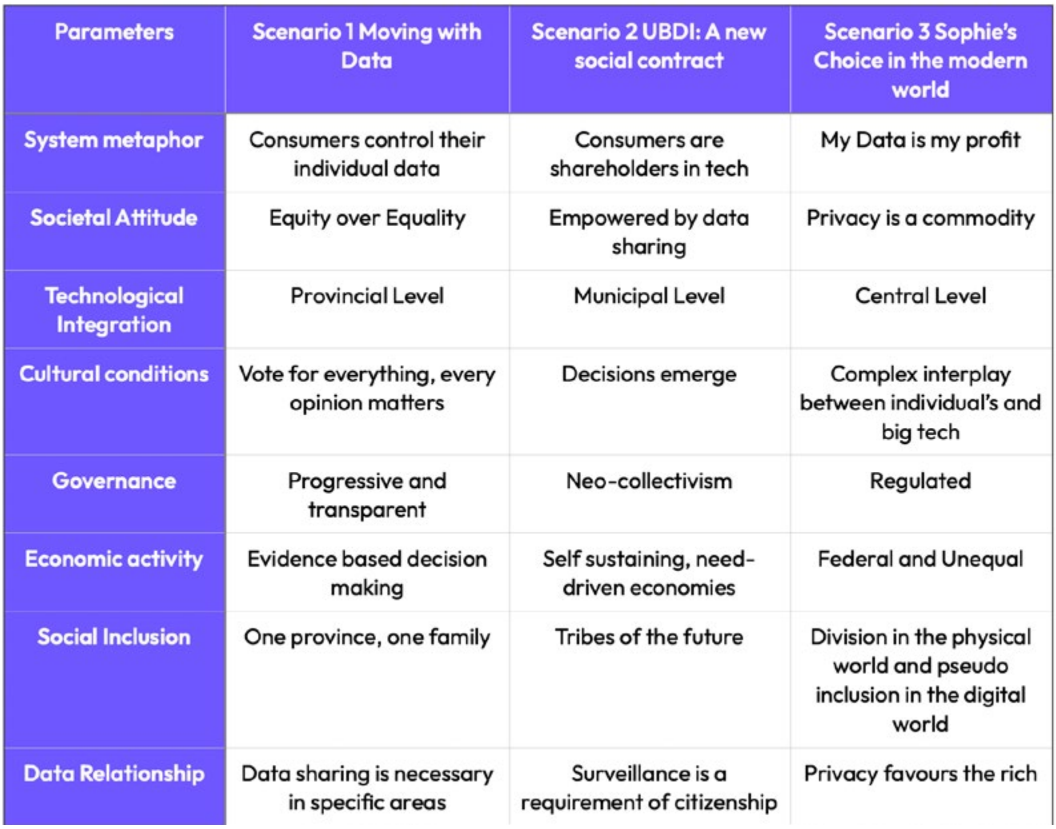
# Creating Alternate Scenarios - The approach

Three alternative future is built upon the current state CLA, where the system levels were deconstructed to identify the different metaphors at the core. The alternative future takes different metaphors and provides distinct viewpoints to initiate a change in the data ecosystem. This new metaphor will then influence the worldview, system causes and the litany of the future state. This project utilizes a foresight lens to explore possibilities for the future. The desired alternative future was developed to encourage flexibility in thinking about the systemic elements that hold us to our current state and to assist with exploratory narratives that may help to challenge and embrace uncertainty (Inayatullah, 2008). As the world changes rapidly, more specifically as the digital platform economy evolves at light speed, alternative futures were specifically explored to imagine a balanced approach. (Hodgson & Sharpe, 2007) In order to improve our capacity to imagine a vastly different future requires understanding the deep system structures that shape our worldview. Therefore, the imagined future shaped by CLA methodology will capture insights, opportunities and barriers to change that may support critical intervention points in supporting ethical data protections and equitable digital futures for all.

# Three alternative future scenarios - summary

This table provides a summary of the three alternative future scenarios included in this section: ‘1. Moving with Data: A Tale of Interoperability and Equity’ ‘UBDI: A new social contract ’, and ‘Sophie’s Choice in the modern world’. The scenarios are differentiated by the ways in which data is governed, the cultural conditions, and technological paradigms. The content in this table is explained in detail within the scenario components.

Table 2 -Three alternative future scenarios summary table



| Parameters | Scenario 1 Moving with Data | Scenario 2 UBDI: A new social contract | Scenario 3 Sophie’s Choice in the modern world |
|---|---|---|---|
| System metaphor | Consumers control their individual data | Consumers are shareholders in tech | My Data is my profit |
| Societal Attitude | Equity over Equality | Empowered by data sharing | Privacy is a commodity |
| Technological Integration | Provincial Level | Municipal Level | Central Level |
| Cultural conditions | Vote for everything, every opinion matters | Decisions emerge | Complex interplay between individual’s and big tech |
| Governance | Progressive and transparent | Neo-collectivism | Regulated |
| Economic activity | Evidence based decision making | Self sustaining, need-driven economies | Federal and Unequal |
| Social Inclusion | One province, one family | Tribes of the future | Division in the physical world and pseudo inclusion in the digital world |
| Data Relationship | Data sharing is necessary in specific areas | Surveillance is a requirement of citizenship | Privacy favours the rich |

# Scenario 1 - Moving with Data: A Tale of Interoperability and Equity

**1. What if the consumers had control and ownership over their data ?**

**2. What if the consumers could choose where to share their data and for what purpose?**

**3. What if the governments use consumer opinion to shape policies and initiatives?**

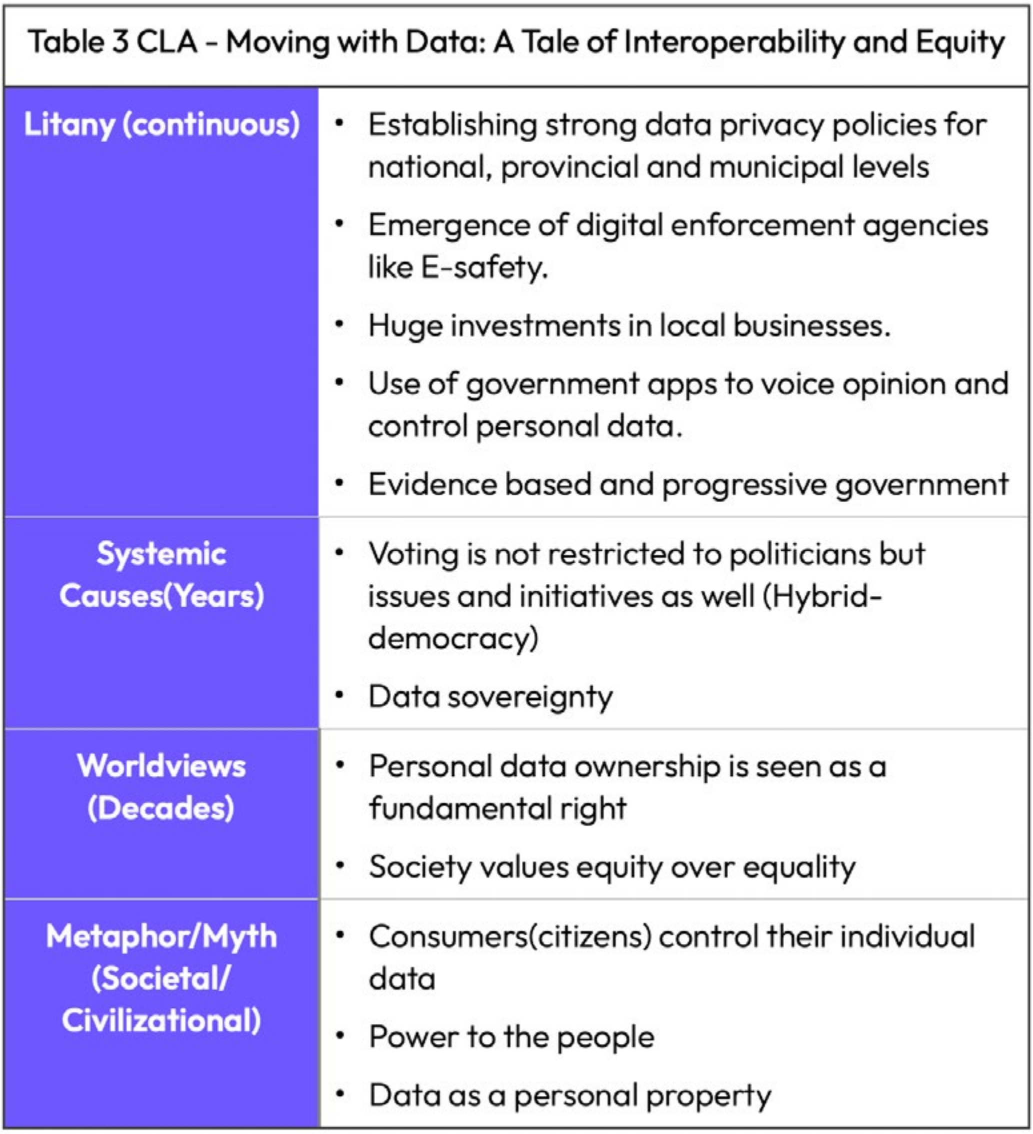


Table 3 CLA - Moving with Data: A Tale of Interoperability and Equity

| | |
|---|---|
| **Litany (continuous)** | • Establishing strong data privacy policies for national, provincial and municipal levels<br>• Emergence of digital enforcement agencies like E-safety.<br>• Huge investments in local businesses.<br>• Use of government apps to voice opinion and control personal data.<br>• Evidence based and progressive government |
| **Systemic Causes(Years)** | • Voting is not restricted to politicians but issues and initiatives as well (Hybrid-democracy)<br>• Data sovereignty |
| **Worldviews (Decades)** | • Personal data ownership is seen as a fundamental right<br>• Society values equity over equality |
| **Metaphor/Myth (Societal/ Civilizational)** | • Consumers(citizens) control their individual data<br>• Power to the people<br>• Data as a personal property |

# Scenario 1 - Moving with Data: A Tale of Interoperability and Equity

It was the year 2040 and the world was a vastly different place. Technology had advanced to the point where AI and algorithms had improved significantly, resulting in the control and influence of big tech increasing to unprecedented levels. With this, data privacy concerns had become more significant than ever before, and the Canadian government had recently enacted a new mandate that data should be controlled by its citizens. This meant that citizens now owned their data, and they were given the authority to decide what they wanted to share. For Mary, a mother of two daughters, this new mandate had a significant impact on her life. Her husband had recently gotten a job offer in British Columbia, which meant that they had to move from their home province of Ontario. However, the fact that her daughters were born in Ontario made it extremely difficult for her to move.

The new data privacy laws had resulted in the collection of personal data becoming increasingly region-specific, which meant that it was difficult to transfer data from one province to another. Mary was worried about how this would impact her and her family's ability to move to British Columbia. Mary decided to reach out to a digital rights advocate who had been fighting for greater interoperability between provinces. The advocate explained to Mary that the new laws had been enacted to give more power to citizens, but that there were still some issues that needed to be ironed out.

Together, they began to lobby for greater interoperability between provinces, arguing that digital rights should be seen as a matter of equity rather than equality. The advocate argued that the current laws disproportionately impacted those who lived in smaller provinces, where the collection of data was less significant. Over time, their lobbying efforts paid off, and the federal government began to pass initiatives that would allow for greater data interoperability between provinces. The provincial government began to conduct and execute those initiatives through data, allowing for greater ease of movement between provinces. In the end, Mary and her family were able to move to British Columbia, and she was able to meet her husband. It was a happy ending, and Mary felt like her efforts had been worth it. She knew that the fight for digital rights would continue, but she was proud of the progress that had been made so far.

## Backcasting: How might we get there?

**2023:** The big tech launches AI systems and advanced algorithms on all platforms and services. The data collection technologies are ubiquitous.

**2025:** The government of Canada notices the influence of big tech and enacts its new digital and data privacy policy that data should be controlled by its citizens

**2027:** The government creates new bodies, compliance and enforcement agencies to facilitate the transition.

**2030:** Consumers support the new policy and register their data on government apps. A strong incentives and investments is directed to small businesses for flourishing Canadian economy and increasing data sovereignty

**2034:** Huge tech companies comply with the laws and enter the Canadian markets. Companies that do not comply are eventually replaced by Canadian tech startups

**2036:** The government starts using digital technology as a way to directly engage with the citizens on new initiatives, issues and decision making.

## Key Drivers of Change

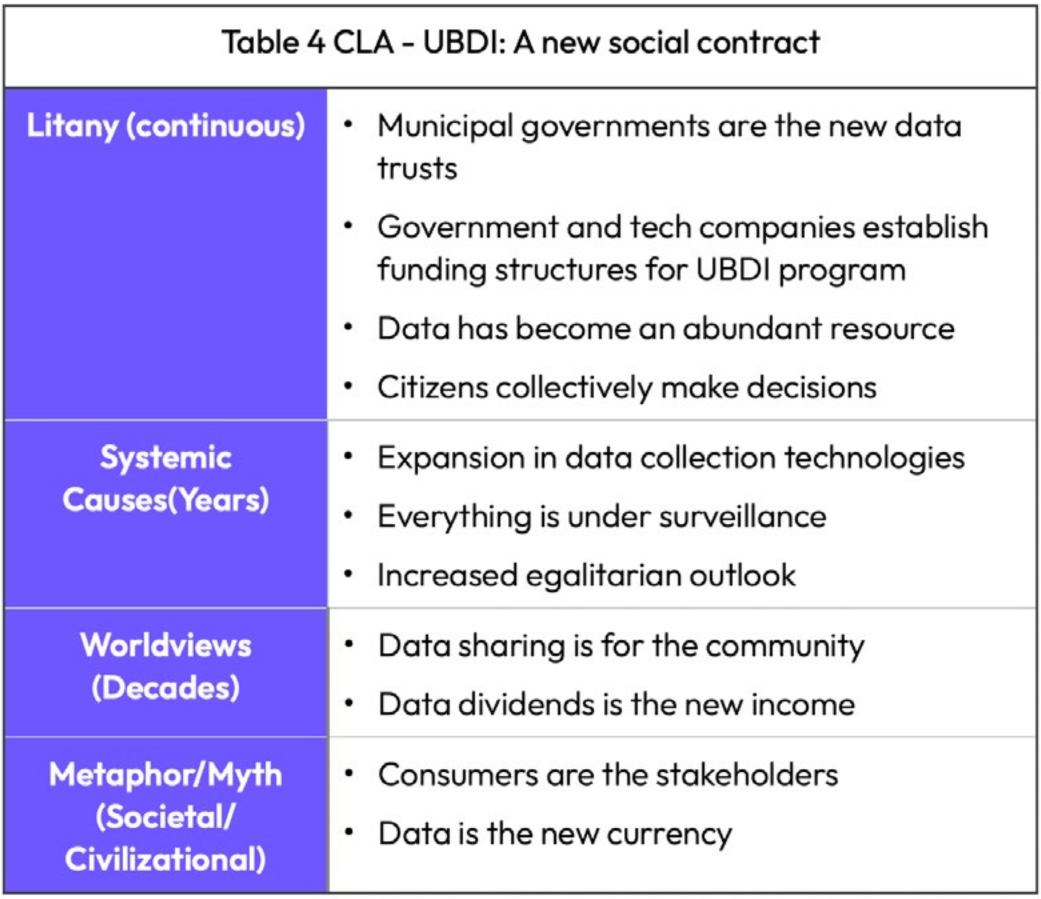
1. The growing influence of big tech
2. The ubiquity of collection of data
3. Shift towards privacy-centric futures

# Scenario 2 - UBDI: A new social contract

**1. What if the consumers had control and ownership over their data?**

**2. What if the consumers could choose where to share their data and for what purpose?**

**3. What if the governments use consumer opinion to shape policies and initiatives?**



| Table 4 CLA - UBDI: A new social contract | |
|---|---|
| **Litany (continuous)** | • Municipal governments are the new data trusts<br>• Government and tech companies establish funding structures for UBDI program<br>• Data has become an abundant resource<br>• Citizens collectively make decisions |
| **Systemic Causes(Years)** | • Expansion in data collection technologies<br>• Everything is under surveillance<br>• Increased egalitarian outlook |
| **Worldviews (Decades)** | • Data sharing is for the community<br>• Data dividends is the new income |
| **Metaphor/Myth (Societal/ Civilizational)** | • Consumers are the stakeholders<br>• Data is the new currency |

## Scenario 2 - UBDI: A new social contract

It was the year 2040 and the world had changed drastically. The effects of climate change had disrupted supply chains, leading to job losses and a struggling economy. To make matters worse, advancements in AI and automation had made many jobs obsolete. To address these challenges, the Canadian government had launched a new policy called Universal Basic Data Income (UBDI). The government realized that data was the new currency of the digital age and that providing citizens with a basic income in exchange for their data would not only stimulate the economy but also help them cope with the job losses.

John was one of the many Canadians who had lost their job due to automation. He was struggling to make ends meet and was grateful for the UBDI policy. He had never thought of his data as a valuable asset, but now he could use it to pay his bills and put food on the table. But the new policy came with a catch. He had register himself at the Municipal Government office to avail the benefits of UBDI. However, the policy had its downsides. In order to qualify for UBDI, citizens had to agree to share their data with the government and its partners. This meant that surveillance was at an all-time high and people were restricted to small communities. It also meant that the government had immense power and control over citizens' data, leading to concerns about privacy and data security. But the new policy came with a catch. Municipal governments were now the new data trusts, and people were restricted to small communities, with surveillance at an all-time high. John felt uneasy about this, but he didn't know what to do. He felt trapped, like he had no choice but to stay in his town.

John was torn between the benefits of UBDI and the loss of his privacy. He had plans to move to the outskirts where there was less surveillance, but he knew that it would be a risky decision. The new social contract had formed, and some people liked it because egalitarian outlooks had emerged, while others didn't like it as they were constantly under surveillance. As John pondered his options, he realized that the UBDI policy was a necessary step to save the economy. He hoped that the government would find a way to balance the benefits of UBDI with the concerns of privacy and data security. Until then, he would have to make a difficult choice between financial stability and personal freedom.

## Backcasting: How might we get there?

**2023:** The big tech launches AI systems and advanced algorithms on all platforms and services. There is also seen a rise in autonomous systems and data collection technologies. Climate change and climate catastrophe are increasing particularly in countries that near to the equator.

**2025:** A large population of people are unemployed due to advancement in AI and machine learning. Climate change has disrupted the supply chain to a significant extend.

**2027:** Canada established measures to cushion the impact of unemployment and disruptions caused by supply chains

**2030:** The Canadian government enacts a social welfare systems called Universal Basic Data Income and puts municipal governments as data trusts to restrict the movement of the citizens.

**2034:** A huge amount of investments is directed towards municipal governments to built financial Infrastructure, data Infrastructure administrative infrastructure and funding infrastructure.

**2036:** Citizens are required to enrol and register at their respective municipal governments to procure UBDI benefits.

## Key Drivers of Change

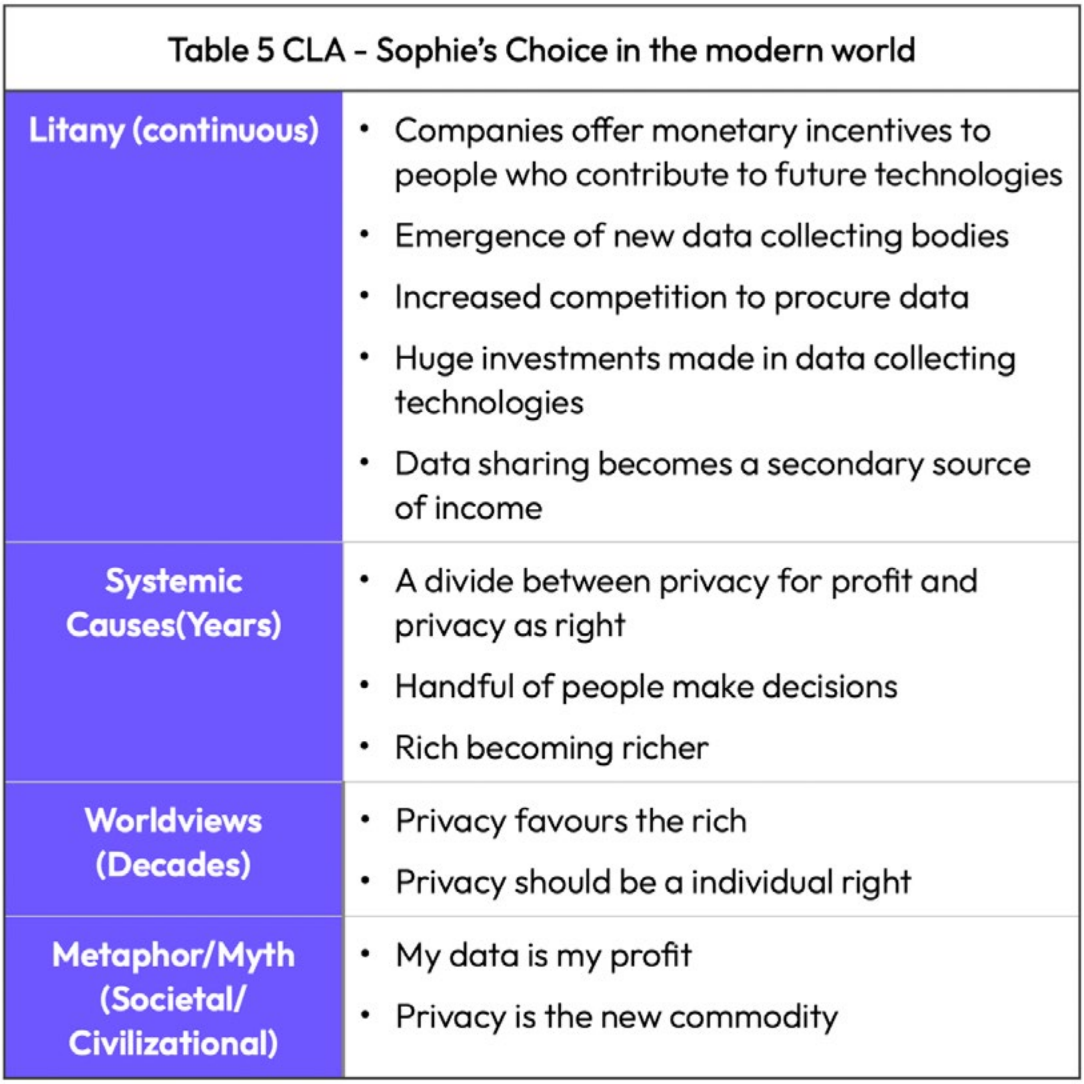
1. Climate change and climate catastrophes
2. Advancement in digital technologies
3. Age of surveillance

# Scenario 3 - Sophie's Choice in the modern world

1. What if the consumers started selling their data to earn more profit?

2. What if big tech companies found a loop hole in Canada's data policy?

3. What if the privacy becomes a commodity?



| Table 5 CLA - Sophie's Choice in the modern world | |
|---|---|
| Litany (continuous) | • Companies offer monetary incentives to people who contribute to future technologies<br>• Emergence of new data collecting bodies<br>• Increased competition to procure data<br>• Huge investments made in data collecting technologies<br>• Data sharing becomes a secondary source of income |
| Systemic Causes(Years) | • A divide between privacy for profit and privacy as right<br>• Handful of people make decisions<br>• Rich becoming richer |
| Worldviews (Decades) | • Privacy favours the rich<br>• Privacy should be a individual right |
| Metaphor/Myth (Societal/ Civilizational) | • My data is my profit<br>• Privacy is the new commodity |

# Scenario 3 - Sophie's Choice in the modern world

Sophie had always been a tech enthusiast, but as the years went by, she became more and more disillusioned with the industry. By 2040, big tech had taken over every aspect of daily life, from social media to healthcare. Sophie was one of the millions who had lost their job to automation and AI. She struggled to make ends meet and had to rely on her savings and the occasional gig economy job to survive. As she scrolled through her newsfeed one day, Sophie stumbled upon an article about a new bill that had just been passed. The Consumer Privacy Protection Act, or Bill C-27, aimed to protect Canadians from big tech's data harvesting practices. Sophie was hopeful at first, but as she read further, she realized that the bill was full of loopholes that allowed companies to continue collecting data as long as they claimed it was for a "legitimate interest."

Sophie knew that this would only make things worse for people like her. Big tech would now have even more power and control over people's data, and the loopholes would make it almost impossible to hold them accountable. As expected, big tech wasted no time in taking advantage of the new legislation. They developed new infrastructure to handle the payment process, systems for tracking and verifying data usage, and established secure and efficient payment channels. They even created a business model to compensate for the data privacy fines they would inevitably incur.

Sophie watched in horror as the world became even more divided. Those who had access to the latest technology and data-sharing platforms thrived, while those who couldn't afford to participate fell further behind. The mental health crisis worsened, as people struggled to cope with the constant surveillance and the feeling of being left behind. Sophie knew she had to do something. She began attending protests and speaking out against the power of big tech. She reached out to other activists and joined forces with them to demand a more equitable and just world.

Despite the odds, Sophie and her allies continued their fight. They knew that the power of big tech was not insurmountable, and that a better future was possible. They continued to push for stronger regulations and more transparency, and eventually, they began to see some progress. Sophie learned that sometimes, the most important thing was to stand up for what you believe in, even when it seemed like the odds were stacked against you. She was proud to be part of a movement that fought for a better future for everyone, not just the privileged few.

## Backcasting: How might we get there?

**2023:** The big tech launches AI systems and advanced algorithms on all platforms and services. There is also seen a rise in autonomous systems and data collection technologies.

**2025:** People started facing mental illness due to lack of employment.

**2027:** The government of Canada passed the Bill C-27 that is Consumer Privacy Protection Act

**2030:** The big tech organisations found a loophole in one of the loosely defined terms in the bill called 'legitimate interest'

**2034:** The big tech started  develop new infrastructure to handle the payment process, systems for tracking and verifying data usage, as well as establishing secure and efficient payment channels.

**2036:** In order to compensate from the data privacy fines, big tech created a business model to take advantage of the bill. A huge divide among people who adopt the change. Protests rise.

## Key Drivers of Change

1. Advancement in digital technologies

2. Corporatocracy

# Analysis and Considerations for moving towards change

## Scenario 1 - Analysis

From this scenario, we can see the importance of data privacy policies that give power to citizens to control their data. There are many positives things which can likely emerge like decision making is a lot more effective, people can actively participate in issues and concerns of nations. However, it also highlights the potential unintended consequences of such policies, such as the difficulty of transferring data between provinces. It is important for policymakers to consider the potential impacts of data privacy policies on individuals and businesses, and to find ways to address any unintended consequences. The scenario also shows the importance of advocacy and lobbying efforts to effect change in government policies. Digital rights advocates play an important role in ensuring that data privacy policies are equitable and not disproportionately impacting certain groups of people.

Furthermore, this scenario highlights the need for interoperability between different regions in terms of data privacy laws. The extent of networks within the global economy, societies, and industries is only partly visible. In a disruption, hidden interdependencies can emerge, unexpectedly accelerating the impact. (*Resilience for Sustainable, Inclusive Growth*, 2022) Although technological integration is at a provincial level, there still needs to be a comprehensive federal policy that unites all the regional policies. This means that policies need to be harmonised and standardised to ensure that data can be easily transferred between different regions without causing unnecessary barriers or difficulties.

## Scenario 2 - Analysis

The scenario of Universal Basic Data Income (UBDI)  highlights the potential benefits and drawbacks of using data as a form of currency. The UBDI policy shows how data can be leveraged to stimulate the economy and support individuals who have lost their jobs due to automation. However, it also demonstrates how the use of data for financial gain can come at the cost of privacy and data security. The scenario also underscores the need for a balance between financial stability and personal freedom. While UBDI offers financial stability, it requires citizens to share their personal data with the government and its partners. This raises questions about who controls the data, how it is used, and the risks associated with data breaches. The scenario suggests that the government needs to find ways to protect citizens' privacy while still harnessing the economic potential of data.

Moreover, the scenario raises concerns about the increasing power and control of the government over citizens' data. This highlights the importance of transparency and accountability in government policies and practices that involve data collection and use. Citizens should have a say in how their data is collected, used, and protected. Overall, the scenario illustrates how the use of data as a currency can have both positive and negative consequences for society, and the need for a balance between economic benefits and privacy concerns. It shows that policies and regulations must evolve alongside technological advancements to ensure that they do not cause harm to citizens.

## Scenario 3 - Analysis

The scenario of Sophie's struggle against big tech highlights the importance of vigilance and advocacy in protecting citizens' privacy and promoting equitable access to technology. It shows that despite the promises of new legislation, corporations will always find loopholes to exploit and maintain their power. Therefore, it is crucial to stay vigilant and advocate for stronger regulations and transparency. The scenario also highlights the potential pitfalls of relying on monetary compensation to address the issue of data privacy. Companies can use such compensation to compensate for the fines they incur, leaving them little incentive to change their practices. Moreover, relying on financial compensation can create further disparities and disconnect in society, as those who can afford to participate in data sharing platforms will continue to thrive while those who cannot will fall further behind or mined or profits.

In addition, the scenario emphasizes the need for governments to stay proactive and take control of big tech before it takes control of them. If left unchecked, big tech can have immense power and influence over governments and societies. Therefore, it is the government's responsibility to create strong regulations and ensure that corporations are held accountable for their actions. This can be done by creating public-private partnerships that ensure that the government has a seat at the table when it comes to shaping the policies of big tech companies. In conclusion, the scenario of Sophie's struggle against big tech serves as a warning about the dangers of unchecked corporate power and the importance of vigilance and advocacy in promoting privacy and equitable access to technology. It also highlights the potential pitfalls of relying solely on financial compensation and underscores the need for proactive government action to control big tech's power and influence.

# Considerations for moving towards change

This section submits three alternative future scenarios that were Moving with Data: A Tale of Interoperability and Equity, UBDI: A new social contract, Sophie's Choice in the modern world. The scenarios were analyze comparatively and the key takeaways are summarized below:

1. The power of big tech companies can be daunting, but collective action and advocacy can help bring about change. Government agencies and local municipalities can act as data trusts and help regulate data collection and usage.

2. In order enforce privacy policies, there needs to be checks and bounces which facilitate ethical collection and protection of data. There is clearly a need of enforcement agencies that pursue legal actions on behalf of citizens.

3. The context and consent plays a huge role in shaping data policies. A nuanced and detailed conversation is needed prior defining terms, compliance and roles of different entities.

4. Public trust in effective data policy deeply depends on the transparency and accountability of the pubic institutions.

5. In the scenarios 3 & 2, monetary compensations by the government or private companies can lead to significant disparities, leading to less personal freedom, more polarisation and lack of trust in public institutions.

6. Effective data policies should take into account the needs and concerns of marginalized communities, rural areas and promote equity and justice for all citizens.

7. Encryption technologies are promising solutions to data privacy, but the state of interoperability remains an area of uncertainty and debate. Arguments for

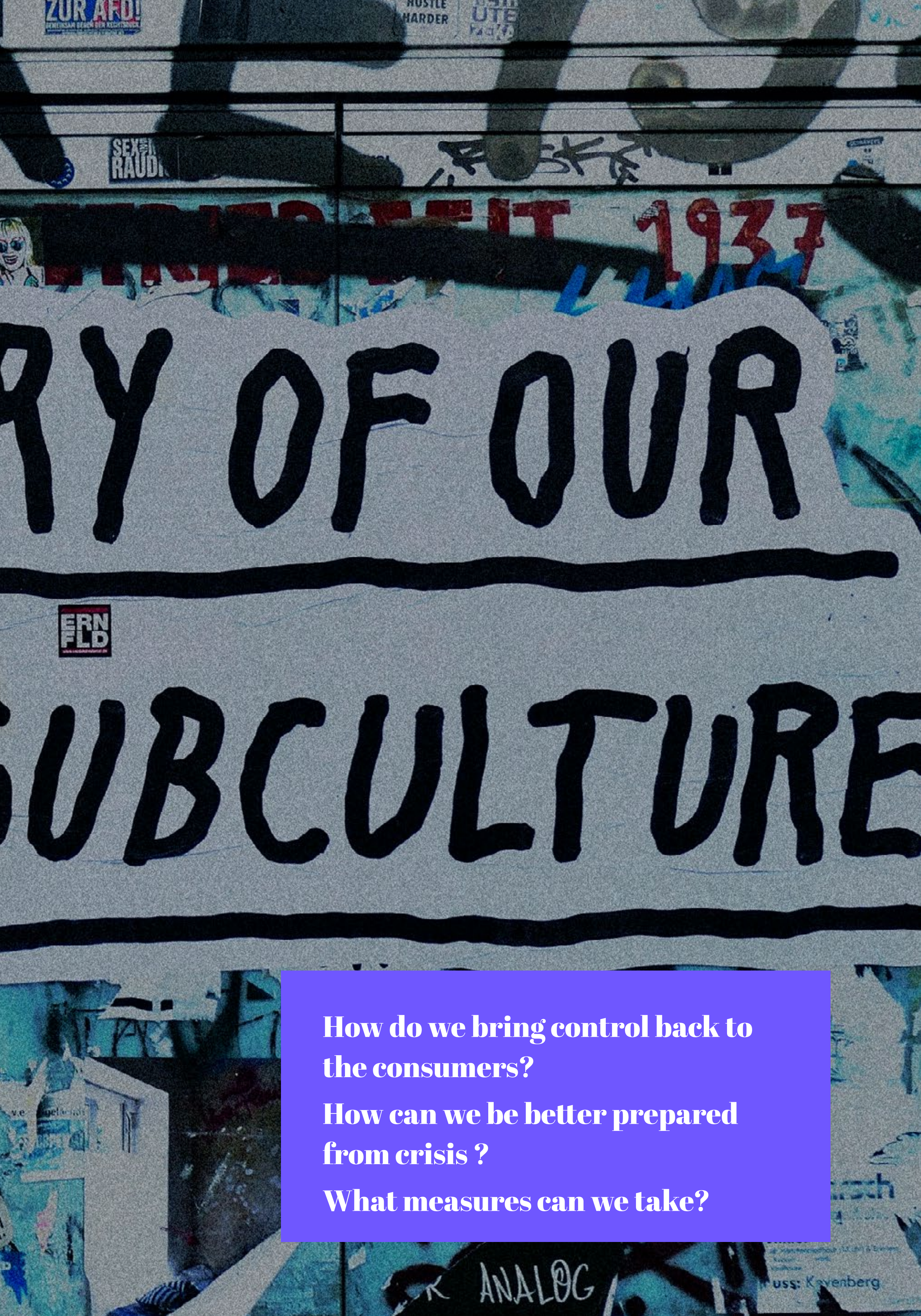
interoperable data systems continue to be met with privacy and cost concerns. It is uncertain how encryption technologies might impact digital governance and future technological innovations.

8. Data privacy policies should consider not only the individuals but small businesses and enterprises that thrive on data generated by other entities. In turn, paying close attention to interoperability and cost of privacy compliance.

9. It is difficult to inform data policies for the upcoming technologies which have not come into the main-stream like advanced algorithms, Artificial General Intelligence(AGI) or web 3. It is highly important to have a stakeholder collaboration towards defining an effective data policy that do not damage the innovation curve.

10. The use of data as currency can stimulate the economy, but it also raises concerns about the ethics of using personal data as a commodity.

# Moving towards change



How do we bring control back to the consumers?

How can we be better prepared from crisis ?

What measures can we take?

# Recommendation 1 : Big change comes from little changes

Given the scope of this research, it is appropriate to provide recommendations that could be applied across data policy initiatives systems and towards defining a ethical data ecosystem

Findings

1. **Data literacy requires digital literacy. A Brookfield Institute study points out that digital literacy is dependent upon infrastructure and internet access, literacy and mathematical skills, economic status, location, educational programs, and a sense of belonging within digital offerings (Huynh & Malli, 2018).**

2. **Canada also has a stark digital divide with rural area internet speeds averaging 5.5 Mbps compared to 50 Mbps speeds in urban centres. (CRTC, 2022)**

3. **Many consumers are aware of the risks associated with sharing their personal information, but they may not have a clear understanding of how their data is being used or who has access to it(Auxier et al., 2020)**

## Action: Increasing data literacy and infrastructure

In addition to educating citizens on data privacy policies, it is equally important to increase the infrastructure that supports privacy protection. Without proper infrastructure, even the most educated citizens can still fall victim to data breaches and unauthorized access. Policymakers should invest in developing secure data storage and transmission systems, as well as in auditing tools that can monitor data usage and alert users of potential breaches. They should also support the development of decentralized data storage systems that allow users to retain control over their data.

To build trust in the public sector and foster future actions, policymakers should prioritize increasing both digital literacy and infrastructure. One effective way to achieve this is by creating online privacy awareness courses that teach privacy basics and provide guidance on best practices for protecting personal data. Policymakers should also implement data privacy education in schools and provide resources to community organizations to educate citizens on data privacy. Furthermore, transparency in tech is equally important to building trust, and policymakers should continuously communicate how personal data is being used and what organizations are using it operationally. By prioritizing education, infrastructure, and transparency, policymakers can empower citizens to take an active role in protecting their personal data and help to create a more trustworthy and sustainable digital ecosystem

# Recommendation 2 : Using change as leverage

Findings

**1. Googlers grappled with unionization, fought against increasing corporate hostility, and challenged their company's unethical partnerships. (Reporter, 2020)**

**2. Tech skeptics are challenging the current paradigm and are working towards developing structures, frameworks, and systems that promote equitable and more humane practices. There are already many students and young professionals readily willing to pursue a career in public interest tech, and plenty of research institutes and academic programs building a bank of knowledge for the sector. (Irwin, 2022)**

**3. Modeled after the framework of public interest law, public interest technology works to ensure technology is designed, deployed, and regulated in a way that protects and improves the lives of people, centering values of equity, inclusion, and accountability where the public interest is at stake. (Public Interest Technology and Its Origins, 2022)**

**4. One of the cons of CPPA is that it places a significant burden on individuals to enforce their privacy rights, as there is no government body dedicated to privacy enforcement. (OpenMedia, 2022) which means individuals should pursue legal actions on their own.**

## Action 1: Hiring Tech Skeptics

With the increasing concern about the impact of technology on society, there has been a rise in the number of tech skeptics advocating for responsible use of technology. Due to war and rising inflation, tech layoffs are at an all time high. (Stringer & Mascarenhas, 2023) Policymakers should take advantage of this trend by creating opportunities for tech experts to contribute to the development of data privacy policies.As the technology industry continues to rapidly evolve, it is becoming increasingly important for governments to have access to the expertise of tech professionals. In order to effectively regulate the technology industry, policymakers need to have a deep understanding of the inner workings of technology and its potential impact on society. The government should establish cells and departments for tech experts who can provide valuable input and insights into the development of regulations and policies related to data privacy. This will help to foster collaboration between policymakers and technology experts, leading to more effective and comprehensive data privacy policies.

## Action 2: Creating New Enforcement Capabilities

In recent years, concerns have been raised about the state of data privacy in Canada. While there are privacy laws in place, there is a lack of enforcement and oversight, which can lead to data breaches and privacy violations going unchecked. To address this issue, there is a growing need for the creation of an independent enforcement agency or privacy body that can monitor and regulate the use of personal data by organizations in Canada. Such a body can work in a similar way to the Food and Drug Administration (FDA) in the United States, which monitors and regulates the safety and efficacy of drugs and medical devices. The establishment of a privacy body would not only ensure that organizations comply with data privacy laws but also build trust among Canadians that their personal data is being used ethically and responsibly.

# Recommendation 3 : Considering small innovations and advocacy

Findings

**1. According to a report by Innovation, Science and Economic Development Canada, small businesses accounted for 98% of all businesses in Canada in 2019. Large businesses, which are defined as those with 100 or more employees, accounted for only 0.2% of all businesses in Canada in the same year(Government of Canada, Statistics Canada, 2022a)**

**2. The CPPA holds all data collecting organizations with high standards, since 98% of Canadian businesses are small businesses, this might raise concerns that the compliance costs associated with the new regulations may be disproportionately burdensome for small businesses with limited resources. (From trends and literature review)**

**3. The power of big tech companies can be daunting, but collective action and advocacy can help bring about change. (From Scenarios)**

**4. Defining 'digital human rights' thoroughly is core of the forming an effective data policy. The context and consent plays a huge role in shaping data policies. A nuanced and detailed conversation is needed prior defining terms, compliance and roles of different entities. (From Scenarios)**

## Action 1: Pregressive Data Tax

In Canada, small businesses play a crucial role in the economy, accounting for nearly 98% of all businesses in the country. However, complying with data privacy regulations can be a significant burden for these small businesses, especially when it comes to the costs associated with implementing the necessary systems and procedures. One potential solution to this issue could be the implementation of a progressive tax system for data privacy compliance, similar to Canada's tax bracket system, where businesses with lower revenue would pay less than larger corporations. The progressive data tax should be based on the amount of collection and processing of data a businesses is responsible for. The implications of high compliance costs for small businesses can be significant. It may lead to reduced innovation, stifling of entrepreneurship, and job losses. In order to address this issue, it is important to explore ways to reduce the compliance burden for small businesses. This would ensure that larger organizations, which have more resources, would pay a larger share of the compliance costs, while smaller businesses would be able to operate with less financial burden. This could help to level the playing field and support the growth and sustainability of small businesses in Canada.

## Action 2: Creating a platform for multi-stakeholder dialogue

As the world becomes increasingly digital, protecting digital human rights is of utmost importance. Policymakers must ensure that citizens have a say in the policies and practices of big tech companies that can impact their lives. To achieve this, policymakers should create a platform for multi-stakeholder dialogue, which brings together representatives from civil society, academia, the private sector, and government.

This platform should provide a forum for open and transparent discussions on digital human rights, data privacy, and other related topics. Through this platform, citizens can voice their concerns and contribute to the development of policies and practices that promote the protection of digital human rights. Additionally, policymakers should ensure that citizens have a seat at the table when it comes to shaping the policies of big tech companies. This will help to ensure that the policies and practices of big tech companies align with the interests and values of citizens, leading to a more sustainable and equitable digital ecosystem.

# Recommendation 4: Preparing for uncertainty

**1. Dozens of countries are exploring military uses of AI. Most research and development happens within the private sector and, critically, many of the most exciting breakthroughs are "dual use" — they have civilian and military applications. (Brands, 2023)**

**2. As individuals' personal information becomes more accessible and potentially vulnerable, there is a risk of identity theft, financial fraud, and other forms of privacy violations.**

**3. Governments and multilateral organizations are pursuing efforts to regulate AI and facial recognition technologies. However, it is uncertain whether these technologies can be controlled given the speed of technological innovation and ubiquity of data collection technologies.**

## Action 1: New Investments

Canada has been a leader in the development of quantum computing technologies, with research and development being conducted at top universities and research centers across the country. In fact, the Canadian government has invested heavily in quantum computing and has launched several initiatives to support research in this field. (Patel, 2022) The Canadian government should remain proactive in its approach to data privacy policies and invest in digital technologies like quantum computing to stay ahead of emerging threats. With the increasing use of advanced technologies in data processing and storage, traditional encryption methods may not be sufficient in protecting sensitive data from sophisticated cyber threats. By investing in quantum computing, Canada can leverage this technology to develop more secure encryption methods and strengthen its data privacy policies. Additionally, the government can collaborate with industry experts and academia to identify emerging threats and design effective policies to mitigate them. Overall, a proactive approach to data privacy policies and investment in advanced technologies can help protect Canadian citizens' personal data from cyber threats and foster trust in the digital economy.

## Action 2: Increasing security

Implementing multi-layered security controls means using a combination of different types of security measures to protect information systems. This approach involves incorporating technical and non-technical security controls to increase the overall security of the system. Firewalls are a technical security control that can prevent unauthorized access to the system by blocking certain types of traffic. Intrusion detection and prevention systems can detect and respond to attacks in real-time. Anti-virus software can prevent malicious code from infecting the system. Data encryption can protect sensitive data by scrambling it so that it can only be read by authorized parties. Access controls, such as passwords or biometric authentication, can restrict access to the system to only authorized users. Employee training can help ensure that employees understand their roles and responsibilities in keeping the system secure and are aware of potential threats and how to respond to them.

By implementing a combination of these different security controls, governments can create a more secure environment that is better protected against cyber threats. Additionally, regular testing and evaluation of these controls can help identify vulnerabilities and areas for improvement, allowing for continual strengthening of the security posture.

# So, what is the future of data privacy policies?

Data privacy has become a significant concern for individuals and organizations in today's digital age. With the proliferation of data breaches, identity thefts, and cyber-attacks, people are becoming increasingly aware of the importance of safeguarding their personal information. As technology advances and data becomes more valuable, the future of data privacy is set to be an ever more important topic. This essay will explore the future of data privacy, including the challenges, opportunities, and potential solutions that will shape the way we protect our data in the years to come.

One of the most significant challenges facing the future of data privacy is the proliferation of connected devices. The Internet of Things (IoT) is rapidly growing, and with it, the number of devices that are connected to the Internet. These devices collect and transmit vast amounts of data, much of which is personal and sensitive. The challenge for the future of data privacy is to find ways to protect this data from being accessed by unauthorized users while still allowing individuals to take full advantage of connected devices' benefits.

Another challenge facing the future of data privacy is the increasing use of artificial intelligence (AI) and machine learning (ML). These technologies are being used to analyze vast amounts of data, including personal information, to identify patterns and trends. While AI and ML can potentially revolutionize many industries, they also pose significant risks to data privacy. For example, AI and ML algorithms can inadvertently reveal sensitive personal information, such as a person's race, religion, or political views, without the individual's knowledge or consent.

Despite these challenges, there are also significant opportunities for the future of data privacy. One of the most promising is the increasing use of encryption technologies. Encryption provides a way to protect data by encoding it so that authorized users can only read it. As encryption technologies become more sophisticated, they will offer a more secure way to protect personal information from being accessed by unauthorized users.

Another opportunity for the future of data privacy is the increasing use of privacy-enhancing technologies (PETs). These technologies aim to enhance data privacy by minimizing the amount of personal information collected and processed. PETs include techniques such as differential privacy, which adds noise to data to make it more difficult to identify individuals, and federated learning, which allows data to be analyzed without being centralized in one location.

In addition to these technological solutions, legal and regulatory measures can help protect data privacy in the future. Many countries have already introduced laws, such as the General Data Protection Regulation (GDPR) in the European Union, that provide individuals with greater control over their personal information. As more countries introduce similar laws, individuals will have more rights and protections regarding their data.

In conclusion, data privacy's future is challenging and full of opportunities. As technology advances, individuals and organizations must find ways to protect personal information from being accessed by unauthorized users while taking full advantage of the benefits that technology offers. Encryption technologies, privacy-enhancing technologies, and legal and regulatory measures will all play an essential role in shaping the future of data privacy. By working together, we can ensure that personal information remains protected in the future.

# Next Steps

The issue of data privacy and ownership has become increasingly important in the digital age, and it is essential to take action to ensure that individuals have control over their personal information. As we have discussed, there is a need for clear and comprehensive policies that protect individuals' data privacy rights while also facilitating innovation and economic growth. The data privacy problem requires a multi-stakeholder approach involving citizens, organizations, and public and private entities to work together to create a system where technology is used for the greater good. Incremental and radical innovation is necessary to move forward, and the government should invest in digital technologies like quantum computing to stay ahead of the curve.

To achieve this, various encryption methods should be considered for different types of data, particularly first-party data, which is highly vulnerable to identity theft. The government should carefully assess the data policy and determine which data sets require what level of encryption. In addition, it is crucial to promote societal literacy in data rights, data privacy, and data transactions to empower individuals to make informed decisions when interacting with data-driven processes and platforms. This can be achieved by creating transparency in how the system operates, instilling trust in the platforms, and implementing clear and robust boundaries for operation.

The digital platform economy and all ecosystem participants will benefit from implementing clear and robust boundaries for operation. This will require global governance frameworks to establish a shared set of values that enable more robust policy and regulation. Regulations should be iterative and flexible to change to keep up with the rapid growth rate of the digital platform economy.

This report serves as a starting point to solve the problems within the digital platform economy. It is crucial to introduce guiding principles into several speculative models that engage multi-stakeholder networks to create a collaborative, low-risk environment for diverse ecosystem participants to co-create ideas around governance frameworks, best practices, and plans for creating education networks centred around data literacy. These speculative models and collaborative practices aim to create systemic change that encourages a tech-enabled future while protecting a tech-centric society. We can create a system that enables a better world with collective efforts and a proactive approach.

# Limitations of Research Study on Data Privacy

Efforts were made to approach this research study comprehensively and holistically. The following limitations are acknowledged following the execution of this report.

### Evolving Landscape

The data privacy policies and digital platform economy today is changing rapidly due to introduction of new regulations (across different countries) and a shift in acceptance of current business operations in society. The growth of the technology sector and platform economy has grown continuously over the last two decades, resulting in inconsistent literature review findings and expert opinions that made defining certain areas of this study challenging.

### Primary Research

This study could benefit from additional participants in the expert interviews. Though the insights from participants were significant, a larger and more diverse participant pool would have allowed for a richer data collection to validate and challenge assumptions. A generative workshop could have facilitated a wider variety of insights in imagining alternative futures. Due to time constraints a larger emphasise was given to literature review.

## Conclusion

Through this research, my objective was to provide privacy-centric think tanks and policy makers a new way of thinking about problems. The consumerism culture gives credible insights about the economy as well as the environment. The emerging shifts on the horizon sheds light on the first order and second order effects. Current and alternate scenarios offers unique perspectives on the problem and imagines news worlds that have merits as well as demerits. Finally the report ends with few recommendations and steps that policy makers can consider to develop ethical practices towards data privacy. Overall the research is built by understanding Canada's digital revolution and upcoming challenges. I hope it engages the readers, provides unique perspectives and encourages new conversations about supporting privacy-centric values through data. The project also demonstrates the potential value of combining designing thinking, systems thinking, and strategic foresight methodology for future research in this field of study.

# References

1. 5 charts showing the jobs of a post-pandemic future – and the skills you need to get them. (2020, October 22). World Economic Forum. https://www.weforum.org/agenda/2020/10/x-charts-showing-the-jobs-of-a-post-pandemic-future-and-the-skills-you-need-to-get-them/

2. A customer-centric approach to marketing in a privacy-first world. (2021, May 20). McKinsey & Company. https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/a-customer-centric-approach-to-marketing-in-a-privacy-first-world

3. About Us - Center for Humane Technology. (n.d.). https://www.humanetech.com/who-we-are

4. Abrams, L. (2021, December 26). Privacy-focused search engine DuckDuckGo grew by 46% in 2021. BleepingComputer. https://www.bleepingcomputer.com/news/technology/privacy-focused-search-engine-duckduckgo-grew-by-46-percent-in-2021/

5. Ai, I. (2019, March 27). Rise Of The Chief Ethics Officer. Forbes. https://www.forbes.com/sites/insights-intelai/2019/03/27/rise-of-the-chief-ethics-officer/?sh=6b3527ce5aba

6. Air, F. (2017, October 26). How 5 Tech Giants Have Become More Like Governments Than Companies. NPR. https://www.npr.org/2017/10/26/560136311/how-5-tech-giants-have-become-more-like-governments-than-companies

7. Akers, B. (2023, March 27). DuckDuckGo Stats on Revenue and User Data Statistics (2023). SEO by Sociallyin. https://seobysociallyin.com/duckduckgo-stats-revenue-and-user-data/

8. Amnesty International. (2021). 'The Great Hack': Cambridge Analytica is just the tip of the iceberg. Amnesty International. https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/

9. Anderson, J., Rainie, L., & Nadeem, R. (2022, September 15). 3. Concerns about democracy in the digital age. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2020/02/21/concerns-about-democracy-in-the-digital-age/

10. Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., Turner, E., & Atske, S. (2020, August 17). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

11. Bank of Canada. (2021, June 10). The digital transformation and Canada's economic resilience. https://www.bankofcanada.ca/2021/06/digital-transformation-canada-economic-resilience/

12. Bass, D. (2019, April 3). Amazon Schooled on AI Facial Technology By Turing Award Winner. Bloomberg.com. https://www.bloomberg.com/news/articles/2019-04-03/amazon-

schooled-on-ai-facial-technology-by-turing-award-winner

13. Benson, T. (2023, January 20). The Small but Mighty Danger of Echo Chamber Extremism. WIRED. https://www.wired.com/story/media-echo-chamber-extremism/

14. Berghel, H. (2018). Malice Domestic: The Cambridge Analytica Dystopia. IEEE Computer, 51(5), 84–89. https://doi.org/10.1109/mc.2018.2381135

15. Bertrand, A. A., & McQueen, J. (2023). Meet the Tech Skeptics. www.ey.com. https://www.ey.com/en_gl/government-public-sector/meet-the-tech-skeptics

16. Big Data and War: Can a Cyberattack Justify an Armed Response? (2023, February 20). UVA Today. https://news.virginia.edu/content/big-data-and-war-can-cyberattack-justify-armed-response

17. Bischoff, P. (2022). Surveillance camera statistics: which cities have the most CCTV cameras? Comparitech. https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

18. Brands, H. (2023, April 5). AI May Be Good for Humanity But Very Bad for Warfare. Bloomberg.com. https://www.bloomberg.com/opinion/articles/2023-04-05/ai-weapons-will-cause-artificial-arms-race-between-us-and-china#xj4y7vzkg?leadSource=uverify%20wall

19. Burgess, M. (2021, March 7). Privacy-First Browser Brave Is Launching a Search Engine. WIRED. https://www.wired.com/story/privacy-first-browser-brave-launching-search-engine/

20. Burgess, M. (2023, February 28). China Is Relentlessly Hacking Its Neighbors. WIRED UK. https://www.wired.co.uk/article/china-hack-emails-asean-southeast-asia

21. CBS News. (2022, October 10). China’s cyber assault on Taiwan - 60 Minutes. CBS News. https://www.cbsnews.com/news/china-cyber-assault-taiwan-60-minutes-2022-10-09/

22. CBS News. (2023, January 4). China’s buildup of the surveillance state — “Intelligence Matters.” CBS News. https://www.cbsnews.com/news/chinas-buildup-of-the-surveillance-state-intelligence-matters/

23. Chart of the Week: The Rise of Corporate Giants. (2018, June 6). IMF. https://www.imf.org/en/Blogs/Articles/2018/06/06/blog-the-rise-of-corporate-giants

24. Cheah, S., & Wang, S. (2017). Big data-driven business model innovation by traditional industries in the Chinese economy. Journal of Chinese Economic and Foreign Trade Studies, 10(3), 229–251. https://doi.org/10.1108/jcefts-05-2017-0013

25. Ciso, E. (2022, October 13). Financial data of over 9M cardholders leaked, including from SBI. ETCISO.in. https://ciso.economictimes.indiatimes.com/news/financial-data-of-

over-9-mn-cardholders-leaked-including-from-sbi-researchers/94826748

26. Collective, T. T. (n.d.). Tactical Tech. https://tacticaltech.org/

27. Concepts. (n.d.). RadicalxChange. https://www.radicalxchange.org/concepts/

28. Crail, C. (2023, February 9). VPN Statistics And Trends In 2023. Forbes Advisor. https://www.forbes.com/advisor/business/vpn-statistics/

29. Data protection in the EU. (2021, June 4). European Commission. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

30. Dickman, H. (2022). The Social Intelligence Report - How it Works. Social Intel. https://www.socialintel.com/how-it-works/

31. Digital Economy Report 2019. (2019, September 4). UNCTAD. https://unctad.org/publication/digital-economy-report-2019

32. Digital Economy Report Pacific Edition 2022. (2023, February 16). UNCTAD. https://unctad.org/publication/digital-economy-report-pacific-edition-2022#:~:text=Digital%20transformation%20is%20under%20way,digital%20payments%20and%20digital%20trade.

33. Fisher, L. (2011, July 25). Social Intelligence offers official social media background checks. TNW | Socialmedia. https://thenextweb.com/news/social-intelligence-offers-official-social-media-background-checks

34. Fussell, S. (2019, September 19). Is Amazon's Search Algorithm Biased? It's Hard to Prove. The Atlantic. https://www.theatlantic.com/technology/archive/2019/09/is-amazons-search-algorithm-biased-its-hard-to-prove/598264/

35. Fussell, S. (2020, November 11). Apps Are Now Putting the Parole Agent in Your Pocket. WIRED. https://www.wired.com/story/apps-putting-parole-agent-your-pocket/

36. Gilliard, C. (2022, October 18). Amazon and the Rise of 'Luxury Surveillance.' The Atlantic. https://www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772/

37. Goldhaber, M. H. (1997, December 1). Attention Shoppers! WIRED. https://www.wired.com/1997/12/es-attention/

38. Goswami, S. (2021, November 23). What The Future Of Consumer Data Ownership Looks Like. Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/11/23/what-the-future-of-consumer-data-ownership-looks-like/?sh=73622fe949e9

39. Government of Canada, Canadian Radio-television and Telecommunications Commission (CRTC). (2023, March 6). Communications Market Reports - Current trends - High-speed broadband. CRTC. https://crtc.gc.ca/eng/publications/reports/policymonitoring/ban.htm

40. Government of Canada, Innovation, Science and Economic Development Canada,

Office of the Deputy Minister, Small Business, Tourism and Marketplace Services & Small Business Tourism and Marketplace Services. (2020, December 10). Key Small Business Statistics — 2020. https://ised-isde.canada.ca/site/sme-research-statistics/en/key-small-business-statistics/key-small-business-statistics-2020#a01

41. Government of Canada, Innovation, Science and Economic Development Canada, Office of the Deputy Minister, Strategy and Innovation Policy Sector & Strategy and Innovation Policy Sector. (2020, March 5). Price Comparisons of Wireline, Wireless and Internet Services in Canada and with Foreign Jurisdictions 2019 Edition. https://ised-isde.canada.ca/site/strategic-policy-sector/en/telecommunications-policy/price-comparisons-wireline-wireless-and-internet-services-canada-and-foreign-jurisdictions-2019

42. Government of Canada, Statistics Canada. (2021a, March 2). The Daily — Gross domestic product by industry, December 2020. https://www150.statcan.gc.ca/n1/daily-quotidien/210302/dq210302b-eng.htm

43. Government of Canada, Statistics Canada. (2021b, April 20). The Daily — Digital supply and use tables, 2017 to 2019. https://www150.statcan.gc.ca/n1/daily-quotidien/210420/dq210420a-eng.htm

44. Government of Canada, Statistics Canada. (2021c, June 22). The Daily — Canadian Internet Use Survey, 2020. https://www150.statcan.gc.ca/n1/daily-quotidien/210622/dq210622b-eng.htm#:~:text=Two%20in%20five%20Canadians%20checked,do%20research%2C%20or%20for%20entertainment.

45. Government of Canada, Statistics Canada. (2022a, January 28). The Canadian Research and Development Pharmaceutical Sector, 2019. https://www150.statcan.gc.ca/n1/pub/11-621-m/11-621-m2022004-eng.htm

46. Government of Canada, Statistics Canada. (2022b, April 28). The Daily — Study: Canadians' use of the Internet and digital technologies before and during COVID-19 pandemic. https://www150.statcan.gc.ca/n1/daily-quotidien/220428/dq220428b-eng.htm#

47. Gratton, É., Joli-Coeur, F., Nagy, A., Du Perron, S., Khoury, D. E., & Vani, M. (2023a). Consumer Privacy Protection Act (Canada's Bill C-27): Feedback from industry participants. BLG. https://www.blg.com/en/insights/2023/01/consumer-privacy-protection-act-canadas-bill-c-27-feedback-from-industry-participants

48. Gratton, É., Joli-Coeur, F., Nagy, A., Du Perron, S., Khoury, D. E., & Vani, M. (2023b). Consumer Privacy Protection Act (Canada's Bill C-27): Feedback from industry participants. BLG. https://www.blg.com/en/insights/2023/01/consumer-privacy-protection-act-canadas-bill-c-27-feedback-from-industry-participants

49. Grimes, D. R. (2018, February 14). Echo chambers are dangerous – we must try to

break free of our online bubbles. The Guardian. https://www.theguardian.com/science/blog/2017/dec/04/echo-chambers-are-dangerous-we-must-try-to-break-free-of-our-online-bubbles

50. Harnessing the potential of data in insurance. (2017, May 12). McKinsey & Company. https://www.mckinsey.com/industries/financial-services/our-insights/harnessing-the-potential-of-data-in-insurance

51. Harwell, D. (2019, August 28). Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns. Washington Post. https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/

52. Higgs, K. (2022, February 24). How the world embraced consumerism. BBC Future. https://www.bbc.com/future/article/20210120-how-the-world-became-consumerist

53. Hill, K. (2019, February 7). I Cut the “Big Five” Tech Giants From My Life. It Was Hell. Gizmodo. https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194

54. Hirsh, M. (2023, April 28). AI-Driven Weapons Systems Lead Today’s Arms Race. Foreign Policy. https://foreignpolicy.com/2023/04/11/ai-arms-race-artificial-intelligence-chatgpt-military-technology/

55. Holloway, D. (2019, June 24). Explainer: what is surveillance capitalism and how does it shape our economy? The Conversation. https://theconversation.com/explainer-what-is-surveillance-capitalism-and-how-does-it-shape-our-economy-119158

56. Home. (n.d.). https://www.oecd-ilibrary.org/sites/9cada708-en/index.html?itemId=/content/component/9cada708-en

57. Iran International. (2023, March 28). Russia, Iran Military Cooperation Expands To Digital Surveillance. Iran International. https://www.iranintl.com/en/202303281993

58. Irwin, V. (2022, May 2). The rise of tech ethicists shows how the industry is changing. Protocol. https://www.protocol.com/workplace/tethics-on-the-rise

59. Isaak, J., & Hanna, M. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. IEEE Computer, 51(8), 56–59. https://doi.org/10.1109/mc.2018.3191268

60. Key Issues Overview - Center for Humane Technology. (n.d.). https://www.humanetech.com/key-issues

61. Kochovski, A. (2023, April 12). The Top 25 VPN Statistics, Facts & Trends for 2023. Cloudwards. https://www.cloudwards.net/vpn-statistics/

62. Lecher, C. (2019, April 25). How Amazon automatically tracks and fires warehouse

workers for ‘productivity.’ The Verge. https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations

63. Lee, G., & Lee, G. (2021, December 20). Fintech cybersecurity: How to keep banking and finance safe in 2022. International Accounting Bulletin. https://www.internationalaccountingbulletin.com/business/fintech-cybersecurity-how-to-keep-banking-and-finance-safe-in-2022/

64. Luxury Surveillance — Real Life. (n.d.). Real Life. https://reallifemag.com/luxury-surveillance/

65. Lystra, T. (2019, May 21). &#8216;All Tech is Human&#8217; event sparks discussion about avoiding unintended consequences of innovation. GeekWire. https://www.geekwire.com/2019/tech-human-event-sparks-discussion-avoiding-unintended-consequences-innovation/

66. Marr, B. (2016, July 26). Are We Heading For Digital-Feudalism In Our Big Data World? Forbes. https://www.forbes.com/sites/bernardmarr/2016/07/26/is-this-the-scary-world-our-tech-revolution-will-create/?sh=295e1a602b96

67. Massachusetts Institute of Technology. (2018, April 10). Amit S. Mukherjee | The Need for ‘Techno-Supporting Skeptics’ | MIT Sloan Management Review. MIT Sloan Management Review. https://sloanreview.mit.edu/article/the-need-for-techno-supporting-skeptics/

68. McBride, J. (2019, May 13). Is ‘Made in China 2025’ a Threat to Global Trade? Council on Foreign Relations. https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade

69. Mission, Team and Story - The Algorithmic Justice League. (n.d.). https://www.ajl.org/about

70. Naughton, J. (2019a, January 20). “The goal is to automate us”: welcome to the age of surveillance capitalism. The Guardian. https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

71. Naughton, J. (2019b, February 17). It’s almost impossible to function without the big five tech giants. The Guardian. https://www.theguardian.com/commentisfree/2019/feb/17/almost-impossible-to-function-without-big-five-tech-giants

72. Naughton, J. (2021, November 21). Can big tech ever be reined in? The Guardian. https://www.theguardian.com/technology/2021/nov/21/can-big-tech-ever-be-reined-in

73. New_ Public - For Better Digital Public Spaces. (n.d.). New_ Public. https://newpublic.org/

74. Nicas, J., Isaac, M., & Frenkel, S. (2021, January 14). Millions Flock to Telegram

and Signal as Fears Grow Over Big Tech. The New York Times. https://www.nytimes.com/2021/01/13/technology/telegram-signal-apps-big-tech.html

75. Nield, D. (2019, June 16). It's Time to Switch to a Privacy Browser. WIRED. https://www.wired.com/story/privacy-browsers-duckduckgo-ghostery-brave/

76. Nycyk, M. (2020). From data serfdom to data ownership: An alternative futures view of personal data as property rights. Journal of Futures Studies, Vol. 24(4)(4), 25–34. https://doi.org/10.6531/JFS.202006_24(4).0003

77. Oaic. (2023, April 18). The Privacy Act. OAIC. https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act#:~:text=The%20Privacy%20Act%201988%20was,other%20organisations%2C%20handle%20personal%20information.

78. Office of the Privacy Commissioner of Canada. (2019, May 31). PIPEDA fair information principles. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

79. OpenMedia. (2022, September 14). The Absolute Bare Minimum: Privacy and the New Bill C-27. https://openmedia.org/article/item/new-bill-C27

80. Our Data Our Selves. (n.d.). Our Data Our Selves. https://ourdataourselves.tacticaltech.org/

81. Our organization is building the Responsible Tech movement — All Tech Is Human. (n.d.). All Tech Is Human. https://alltechishuman.org/about

82. Patel, N. (2022, August 15). These Canadian startups are taking quantum computing mainstream. CBC. https://www.cbc.ca/news/business/quantum-computers-canada-1.6546128

83. Pegg, D., & Cutler, S. (2021, July 20). What is Pegasus spyware and how does it hack phones? The Guardian. https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

84. Peters, K. (2022). What Is Universal Basic Income (UBI), and How Does It Work? Investopedia. https://www.investopedia.com/terms/b/basic-income.asp

85. Public interest technology and its origins. (2022, June 3). Ford Foundation. https://www.fordfoundation.org/work/challenging-inequality/technology-and-society/public-interest-technology-and-its-origins/

86. RadicalxChange. (n.d.). RadicalxChange. https://www.radicalxchange.org/

87. Report: Russia Provides Iran With Digital Surveillance Capabilities. (2023, March 29). IranWire. https://iranwire.com/en/technology/115074-report-russia-provides-iran-with-digital-surveillance-capabilities/

88. Reporter, G. S. (2020a, April 16). What we learned from over a decade of tech activism. The Guardian. https://www.theguardian.com/commentisfree/2019/dec/22/tech-worker-activism-2019-what-we-learned

89. Reporter, G. S. (2020b, April 16). What we learned from over a decade of tech activism. The Guardian. https://www.theguardian.com/commentisfree/2019/dec/22/tech-worker-activism-2019-what-we-learned

90. Research, S. (n.d.). GDPR Services Market New Research Analysis and Forecast 2030. https://straitsresearch.com/report/gdpr-services-market

91. Resilience for sustainable, inclusive growth. (2022, June 7). McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/resilience-for-sustainable-inclusive-growth

92. Rice, M. (2019). 21 Big Data Insurance Companies to Know. Built In. https://builtin.com/big-data/big-data-insurance

93. Rising demand for data protection officers. (n.d.). Reuters. http://fingfx.thomsonreuters.com/gfx/rngs/CYBER-GDPR-DPO/010060WY1RF/index.html

94. Robles, P. (n.d.). China plans to be a world leader in Artificial Intelligence by 2030. South China Morning Post. https://multimedia.scmp.com/news/china/article/2166148/china-2025-artificial-intelligence/index.html

95. Rodriguez, J., & Rodriguez, J. (2019, December 19). “We’re sorry”: 15M LifeLabs customers may have had data breached in cyberattack. CTVNews. https://www.ctvnews.ca/health/we-re-sorry-15m-lifelabs-customers-may-have-had-data-breached-in-cyberattack-1.4733963

96. Rodriguez, S. (2018, February 14). Rise of the data protection officer, the hottest tech ticket in town. U.S. https://www.reuters.com/article/us-cyber-gdpr-dpo/rise-of-the-data-protection-officer-the-hottest-tech-ticket-in-town-idUSKCN1FY1MY

97. Seetharaman, D. (2019, July 26). New Netflix Documentary on Cambridge Analytica Doubles as a Mystery. WSJ. https://www.wsj.com/articles/new-netflix-documentary-on-cambridge-analytica-doubles-as-a-mystery-11564146036

98. Seneca, C. (2020, September 17). How to Break Out of Your Social Media Echo Chamber. WIRED. https://www.wired.com/story/facebook-twitter-echo-chamber-confirmation-bias/

99. Solon, O. (2018, February 14). Amazon patents wristband that tracks warehouse workers’ movements. The Guardian. https://www.theguardian.com/technology/2018/jan/31/amazon-warehouse-wristband-tracking

100. SOMO. (2022). How Big Tech is becoming the Government. SOMO. https://www.

somo.nl/how-big-tech-is-becoming-the-government/

101. Specht, D. (2019, June 6). Tech companies collect our data every day, but even the biggest datasets can't solve social issues. The Conversation. https://theconversation.com/tech-companies-collect-our-data-every-day-but-even-the-biggest-datasets-cant-solve-social-issues-118133

102. Staff, R. (2019, December 17). LifeLabs hack may have compromised personal info of 15 million Canadians. U.S. https://www.reuters.com/article/us-canada-health-cyber-idCAKBN1YL2KX

103. Stringer, A., & Mascarenhas, N. (2023, April 27). TechCrunch is part of the Yahoo family of brands. https://techcrunch.com/2023/04/27/tech-industry-layoffs/

104. Suciu, P. (2020, June 26). There Isn't Enough Privacy On Social Media And That Is A Real Problem. Forbes. https://www.forbes.com/sites/petersuciu/2020/06/26/there-isnt-enough-privacy-on-social-media-and-that-is-a-real-problem/?sh=5fafe68544f1

105. TechCongress: A Congressional Innovation Fellowship. (2023, April 14). TechCongress. https://www.techcongress.io/

106. TechCrunch is part of the Yahoo family of brands. (2019a, January 30). https://techcrunch.com/2019/01/30/state-bank-india-data-leak/

107. TechCrunch is part of the Yahoo family of brands. (2019b, November 2). https://techcrunch.com/2019/11/02/twitters-political-ads-ban-is-a-distraction-from-the-real-problem-with-platforms/

108. TechCrunch is part of the Yahoo family of brands. (2020, October 21). https://techcrunch.com/2020/10/21/mine-series-a/

109. The consumer-data opportunity and the privacy imperative. (2020, April 27). McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

110. The rise of Data Capitalism - Trinità dei Monti. (2021, July 31). Trinità Dei Monti. http://trinitamonti.org/2021/02/28/the-rise-of-data-capitalism/

111. The rising importance of data ethics. (n.d.). Deloitte. https://www2.deloitte.com/ca/en/pages/deloitte-analytics/articles/the-rising-importance-of-data-ethics.html

112. Usercentrics. (2023). Japan Act on the Protection of Personal Information (APPI): An Overview. Consent Management Platform (CMP) Usercentrics. https://usercentrics.com/knowledge-hub/japan-act-on-protection-of-personal-privacy-appi/#:~:text=of%20personal%20information.-,What%20is%20the%20Act%20on%20the%20Protection%20of%20Personal%20Information,agencies%2C%20businesses%2C%20and%20nonprofits.

113. Waddell, K. (2021, February 24). Tech companies too secretive about algorithms

that curate feeds, study says. Consumer Reports. Retrieved April 25, 2023, from https://www.consumerreports.org/consumer-protection/tech-companies-too-secretive-about-algorithms-that-curate-feeds-a8134259964/

114. Wallach, O. (2021, July 9). The World's Tech Giants, Compared to the Size of Economies. Visual Capitalist. https://www.visualcapitalist.com/the-tech-giants-worth-compared-economies-countries/

115. Wang, X., & Xu, M. (2018). Examining the linkage among open innovation, customer knowledge management and radical innovation. Baltic Journal of Management, 13(3), 368–389. https://doi.org/10.1108/bjm-04-2017-0108

116. Who We Are - The Psychology of Technology Institute — Psychology of Technology Institute. (n.d.). Psychology of Technology Institute. https://www.psychoftech.org/about

117. Wisevoter. (2022, October 20). Should the government break up large tech companies? - Wisevoter. https://wisevoter.com/issue/big-tech/

118. Witt, S. (2022, December 12). The World-Changing Race to Develop the Quantum Computer. The New Yorker. https://www.newyorker.com/magazine/2022/12/19/the-world-changing-race-to-develop-the-quantum-computer

119. Wong, J. C. (2020, December 15). Twitter to ban all political advertising, raising pressure on Facebook. The Guardian. https://www.theguardian.com/technology/2019/oct/30/twitter-ban-political-advertising-us-election

120. Wpengine. (2022, November 11). Canada's Digital Divide and the Path to Digital Equity for All Ages - Samuel Centre For Social Connectedness. Samuel Centre for Social Connectedness. https://www.socialconnectedness.org/canadas-digital-divide-and-the-path-to-digital-equity-for-all-ages/

121. Wu, D. (2022, November 1). Inside China's Surveillance State, Built On High Tech And A Billion Spies. Worldcrunch. https://worldcrunch.com/culture-society/china-surveillance-cameras

122. Yahoo is part of the Yahoo family of brands. (n.d.-a). https://news.yahoo.com/russia-supplies-iran-cyber-weapons-222100299.html

123. Yahoo is part of the Yahoo family of brands. (n.d.-b). https://news.yahoo.com/britain-more-surveillance-cameras-per-151641361.html

124. Yahoo is part of the Yahoo family of brands. (n.d.-c). https://ca.finance.yahoo.com/news/global-consent-management-platforms-market-111400345.html

125. Yohn, A. (2023, March 23). 2023 Trends for Data Analytics in Insurance. Duck Creek. https://www.duckcreek.com/blog/predictive-analytics-reshaping-insurance-industry/

126. Zarkadakis, G. (2021, June 27). How selling our personal data can fund universal

basic income. Fortune. https://fortune.com/2021/06/27/universal-basic-income-data-privacy-trusts/

127. Zheng, S. (2023, February 14). Worse Than Spy Balloons? Taiwan Is More Concerned With Chinese Hacking. Bloomberg.com. https://www.bloomberg.com/news/newsletters/2023-02-14/spy-balloons-no-match-for-china-s-cyber-attacks-suggests-taiwan

## Images

Photo by [Annie Spratt](https://unsplash.com/@anniespratt?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) on [Unsplash](https://unsplash.com/photos/t859lVr8KY0?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText)

Photo by [Jingxi Lau](https://unsplash.com/@imajingation?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) on [Unsplash](https://unsplash.com/photos/Y5oVH2tNN9U?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText)

Photo by cottonbro studio: [https://www.pexels.com/photo/group-of-people-in-white-shirts-8088443/](https://www.pexels.com/photo/group-of-people-in-white-shirts-8088443/) - pexels - present

Photo by [Brxxto](https://unsplash.com/@brxxto?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) on [Unsplash](https://unsplash.com/photos/XRd3VwizjUk?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText)

Photo by [JOHN TOWNER](https://unsplash.com/@heytowner?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) on [Unsplash](https://unsplash.com/photos/bZXQ6zUmqkw?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) - emerging shifts

Photo by [VIRUL](https://unsplash.com/@virul?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) on [Unsplash](https://unsplash.com/photos/cM-rZb3PbDc?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) - shift to privacy

[https://www.science.org/content/article/quantum-computers-take-key-step-toward-curbing-errors](https://www.science.org/content/article/quantum-computers-take-key-step-toward-curbing-errors) tech race

Photo by [Etienne Girardet](https://unsplash.com/@etiennegirardet?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) on [Unsplash](https://unsplash.com/photos/CxTCcjUo2hM?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText)

https://www.unicef.org/mena/stories/5-tips-children](https://www.unicef.org/mena/stories/5-tips-children) unicef

Photo by [fikry anshor](https://unsplash.com/ja/@fikry_anshor?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) on [Unsplash](https://unsplash.com/photos/znZFuVcGen4?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText)

A project submitted to OCAD

Futures of Data Ownership by Vinit Soneji

SFI 2023