May 2023

# Amending Amendments: Digital Colonialism, Bill C-11, and Assessing the Call for Improvement

Kayla Victoria Destiny Clarke
*University of Windsor*, clarke27@uwindsor.ca

# *Amending Amendments:* Digital Colonialism, Bill C-11, and Assessing the Call for Improvement

By:

**Kayla Clarke**

A Major Research Paper
Submitted to the Faculty of Graduate Studies Through the Department of Communication, Media and Film in Partial Fulfillment of the Requirements for The Degree of Master of Arts at the
University of Windsor

Windsor, Ontario, Canada

2023

***Amending Amendments:*** **Digital Colonialism, Bill C-11, and Assessing the Call for Improvement**

by

Kayla Clarke

APPROVED BY:

_____

K. Asquith
Department of Communication, Media and Film

_____

V. Manzerolle, Advisor
Department of Communication, Media and Film

April 26, 2023

## DECLARATION OF ORIGINALITY

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis and have included copies of such copyright clearances to my appendix.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

## ABSTRACT

Media scholars Nick Couldry and Ulises Mejias (2019) define digital colonialism as the "term for the extension of a global process of extraction that started under colonialism and continues through industrial capitalism, culminating in today's new form: instead of natural resources in labor, what is now being appropriated is human life through its conversion into data" (p. 22). This research will critically analyze the Canadian government's ill-received Bill C-11: the Amended Consumer Privacy Protection Act by using digital colonialism as a conceptual framework to reveal the Bill's essential limitations. It will consist of two sections: 1) an in-depth exploration of the definition of digital colonialism and Indigenous Subjectivity, which will inform the objective, and 2) an examination of amendment recommendations (7, 8, 11 and 15), put forth by the previous Privacy Commissioner Daniel Therrien to improve Bill C-11. By using digital colonial theory and applying it to a critical legislative case study, this research addresses the following questions: What is digital colonialism and how, from a digital colonial standpoint, can we critically unpack the recommended amendments proposed by Therrien?



**Keywords:** digital colonialism, Bill C-11, consumer, Therrien, Indigenous subjectivity, decolonization, decoloniality, colonizers, prosumer, data, labour exploitation, consent, domination, dispossession, extraction

## DEDICATION

I dedicate this paper to my parents, friends and family, namely my mum Marcia, dad Roydell, sister Shawnté, friends Duck, Djenny, Jessica, and Zee who were there every step of the way. You have supported me through my highs, my extreme lows, and everything in between. I could not have done this without you.

## ACKNOWLEDGEMENTS

Here’s to my colleagues, Samantha, Emily, Shane, and Mackenzie, whose drive and success pushed me to persevere, even if they didn’t know.

Here’s to my integral professors, Dr. Manzerolle, Dr. Asquith, and Dr. Scatamburlo-D'Annibale, some of whom I have known since first-year when I was 19-years-old. You all are constant inspirations to me. Thank you so much.

## TABLE OF CONTENTS

## GLOSSARY

**Colonialism -** Colonialism refers to the exploitative economic, political, and social conquering of the Third World by Settler colonies (Kohn & Kavita, 2017).

**digital colonialism –** The digital extension of Colonialism, in which data is appropriated to the benefit of the digital colonizers.

**Extractees -** The term extractees refers to those whose data is extracted and sold by Big Tech corporations such as IBM., Facebook, Google, Amazon, etc. It also refers to the colonized populations during Colonialism. In Bill C-11, the extractees are referred to as consumers.

**Flak -** In the context of this MRP, flak refers to the widespread, bi-partisan critique the Government of Canada's Bill C-11 received for several shortcomings.

**Four Actors of Digital Colonialism -**

*Actor 1: Technology corporations*

*Actor 2: Consultant and advertising businesses*

*Actor 3: The local parties and governmental organizations*

*Actor 4: The extractees*

**Organizations –** This legislative term refers to the companies who extract and sell consumer data, usually known as governments or corporations. In Bill C-11, the governments and corporations are referred to as organizations.

## IMPORTANT NOTE:

The term "Colonialism" with the capital C, refers to historical, traditional colonialism.

## LIST OF ABBREVIATIONS

**AI -** Artificial Intelligence

**CCLA** - Canadian Civil Liberties Association

**CSA -** Canadian Standards Association

**CPPA -** Consumer Privacy Protection Act

**ETHI** - House of Commons Standing Committee on Access to Information, Privacy and Ethics

**IBM -** International Business Machines Corporation

**ICANN -** Internet Corporation for Assigned Names and Numbers

**ICT -** Information and Communications Technolog(ies)

**IoT -** Internet of Things

**MRP -** Major Research Paper

**OECD -** Organization for Economic Co-operation and Development

**OPC -** Office of the Privacy Commissioner

**OCAP -** Ownership, Control, Access, and Possession

**PIPEDA -** Personal Information Protection and Electronic Documents Act

**TPP -** Free Trade Agreements the Trans Pacific Partnership

**TTIP -** Transatlantic Trade and Investment Partnership

**TISA -** Trade in Services Agreement

**UNDRIP -** United Nations Declaration on the Rights of Indigenous Peoples

## INTRODUCTION

*"The problem is not only about dependency on a foreign provider or applicable laws to digital data; the problem is also about the absence of public policies to address the issue at all levels. The situation of digital domination, close to Colonialism[1], still fails to fill the top priorities of the global political agenda. Almost forty years after the invention of the Internet, the ability of politicians and social leaders to understand the dimensions of the problem still falls short."*

*Renata Avila Pinto on Digital Colonialism, 2021, p. 21*

It has been two decades since the last governmental attempt to modernize Canada's broadcasting, privacy and consumer protection legislation. According to Alberta's Privacy Commissioner Jill Clayton, in comparison to other regulatory jurisdictions like the European Union, Canadian digital legislation amendment is long overdue (Warburton, 2021). In 2020, the Liberal government under Prime Minister Justin Trudeau proposed new legislation to address Canada's outdated policies, resulting in a two-part Act—Bill C-11—to 1) enact the Consumer Privacy Protection Act and 2) to enact the Personal Information and Data Protection Tribunal Act as a part of their Digital Charter Implementation Act (Office of the Privacy Commissioner, n.d). As of spring 2023, Bill

[1] Colonialism, in this context, refers to the exploitative economic, political, and social conquering of the Third World by Settler colonies. This definition acknowledges that Colonialism is not only historical, as its effects continue to manifest today. Colonialism is generally defined as the non-imperial "practice of domination, which involves the subjugation of one people to another" (Kohn & Kavita, 2017).

C-11 is still being questioned on various platforms, from the House of Commons to Twitter.

Bill C-11 was proposed to protect Canadian consumers from the issues that arise from a lack of data security, such as meaningful consent, de-identification, and data mobility (Parsons, 2021). Specifically, Bill C-11, the updated Consumer Privacy Protection Act (CPPA), "introduced new legislation for the collection, distribution, use and disclosure of personal information for commercial activity in Canada" in which its updates would repeal outdated sections of the Personal Information Protection and Electronic Documents Act (PIPEDA) (User Centrics, 2021, para. 3). While a step in the right direction, Bill C-11 "died on the order paper" meaning it was unable to pass prior to, and because of the election call in August of 2020. Since Bill C-11, at the time, did not have the chance to reach the House of Commons' committee study, the overall loss in legislative progress was minimal (Aiello, 2023). However, while the Bill is set to reach the House in 2023, strongly critical discourse continues more than two years later as many Canadian academics take issue with Bill C-11.

Some of these issues were explored by the Canadian public broadcaster CBC. In an article titled "New privacy bill won't fix Canada's longstanding issues," the CBC reported that there were many critics and skeptical scholarly experts who were not only unsurprised by the extensive political critique Bill C-11 received, but they deemed the critique it was receiving justified (Warburton, 2021). The previous Privacy Commissioner Daniel Therrien[2] felt so strongly about the shortcomings of the bill that he

[2] Daniel Therrien was the 8th Privacy Commissioner of Canada. Prior to being politically appointed Commissioner in 2014, he served as a passionate human rights lawyer for over 30 years. Therrien has advocated for the privacy rights of Canadians on all fronts, but most of his most prominent cases focus on Canadian digital privacy. Since assuming office, Therrien has fought for rightful legislation regarding the

claimed it "represented a step backward from current private sector legislation" (Therrien, 2021, para. 12). In addition to this, Therrien submitted a detailed document of recommended improvements for the amendment of the Bill, as requested by the Government of Canada (Therrien, 2021, para. 12). Because of this, Therrien sent the House of Commons Standing Committee on Access to Information, Privacy and Ethics a total of 60 recommendations for Bill C-11's improvement, which included concerns for Bill C-11's treatment of control, accountability, responsible innovation, and access to quick and effective remedies (Therrien, 2021). My paper highlights the shortcomings of Bill C-11 addressed by Therrien while using the theoretical framework of digital colonialism to reframe the most significant proposed amendments.

Like traditional understandings of Colonialism, data extraction by big corporations has caused irreparable damage to the world. Griziotti (2018), an Italian digital engineer, discussed the irreparable damage caused by digital colonialism by exploring what he likes to call e-waste, the second most wasteful resource in the world. Griziotti explains that the environmental degradation that resulted from labour exploitation during Colonialism is also present in digital colonialism. However, it is evident in a neurological way. He states that "this type of pollution is created through a situation of continual fear exerted by a government in a perennial "state of exception," by the extension of workplace stress into life" (p. 104). He also explains that "the policy of precarity implemented in the name of competitiveness contributes to an environment of anxiety, as biohypermedia is his main unit of analysis. This environment produces

cyberbullying bill, the RCMP's access to information, consumers rights, and privacy within the private and public sectors. In 2020, Therrien's office was asked to review and present improvements to Bill C-11 (Chartered Professional Accountants Canada, n.d).

diseases that create an interesting ‘market’ where containment activities and symptomatic care are developed” (p. 104).

Since data production requires tangible resource-intensive extraction, “the rhetoric of ongoing exponential increases in data collection to fuel surveillance-driven models of platform capitalism is revealed to be little more than the latest colonial-capitalist fantasy” (Taffel, 2021, p.11). In their article, Taffel (2021) explains that

> Rethinking the metaphor ‘data is the new oil’ should draw parallels between the injustices associated with colonial and postcolonial extractions of geological wealth and data colonialism’s extraction of contemporary wealth. In both cases, powerful corporate actors argue that they alone possess the means to extract valuable raw materials and refine them into commodities that will allegedly benefit humanity, but which actually only enrich economic elites, increase economic inequality, and cause significant ecological harm (p. 5).

When resources like oil or personal data are labeled the most profitable resource, companies ignore the ecological impact to fight for ownership (Couldry & Mejias, 2019). Additional examples and anecdotes of this manifestation will be further discussed in the section on defining digital colonialism. However, academics Mouton and Burns (2021) postulate that, as researchers, the ache to analyze with specific frameworks is a result of the idea that “as the 'datafication' of our daily lives progresses and attracts mounting attention in academic realms, scholars find themselves in need of new conceptual tools to make sense of the latest developments in data-intensive forms of capitalism” (p. 1892). The assertion that there is a conceptual framework missing from legislation provides the basis for my research, as I will address this gap through the lens of digital colonialism.

In an expert panel that took place in late 2020, Canadian digital protection experts including Scassa, Laidlaw, Gratton, Cofone, and Geist predicted the reasons for Bill C-11's shortcomings. They did this by addressing themes that fall within the analytic purview of digital colonialism without explicitly using the term (Towards a New Privacy Deal? Hot Takes from Privacy Experts on C-11). I speculate that the reason for its address without the specific label is due to the negative connotation of the word "Colonialism," and the fact that the theoretical framework that is digital colonialism is an ambivalent term with multiple definitions. The information discussed at the University of Ottawa's Centre for Law, Technology and Society panel as well as my extensive critical discourse analysis, has led me to identify digital colonialism as a useful framework for Bill C-11's shortcomings. Furthermore, it has led me to identify digital decoloniality,[3] the dismantling of Colonial regimes, as a solution to the problems of digital colonialism.

In this paper, I question the policy's shortcomings by employing digital colonialism as a core analytic framework. However, I will not be developing my own critiques; rather I will highlight four of Therrien's suggestions that address digital colonial articulations of power such as the logic of extraction, domination[4], and exploitation. Building on these articulations, this major research paper will use the term digital colonialism to examine the shortcomings of Bill C-11. The objective is to

[3] "Decoloniality is therefore not simply decolonization, defined as the end of colonial occupation and administration, but a broader rethinking of relations to ongoing coloniality. As postcolonial theorists themselves pointed out, decolonization did not result in the liberation of subjugated peoples but in the continuity of domination through new forms (including, as we argue in this book, in new social relations managed through data)" (Couldry & Mejias, 2019, p. 80).

[4] Domination implies a one-sided endeavour, in which collaboration was not an option or the actors doing the dominating knew that the other side would be opposed to the idea, and therefore they removed the choice. In layman's terms, it is the idea that settler colonialism "destroys to replace" (Wolfe, 2006, p. 388).

understand the limitations of this legislation by examining one of the Bill's official critiques through a digital colonial lens.

## Bill C-11 Background

While quite extensive, Canada's digital privacy protection laws do not have the best track record in terms of update consistency and modernization. Before the tabling of Bill C-11 in the Fall of 2020, Canada had not undergone regulatory changes to the Digital Charter Protection Act in almost two decades. However, digital privacy laws more generally had undergone considerable revisions that had left the country in a digital legislative state of 'work-in-progress.'

The Personal Information Protection Electronic Documents Act (PIPEDA) was implemented in 2000. The principles that inform the purpose and operation of PIPEDA stemmed from the guidelines of the Organization for Economic Co-operation and Development (OECD) in 1981. In 1996, these guidelines were adapted by the Canadian Standards Association (CSA) then officially adopted into Canadian federal private sector regulation in 2000 (Phull, 2019). Since then, there has been "the federal government's introduction of a Digital Charter (2018), the parliamentary report Towards Privacy by Design (2018), and proposals and guidelines such as "Strengthening Privacy for the Digital Age" and "Guidelines for obtaining meaningful consent" (Kavya, 2021). These reports represent governmental action that should have led to Bill C-11. It is difficult to follow the path and timeline of digital privacy legislation in Canada as there have been dozens of proposals to update the outdated policies from different political parties. While commendable, there has still been little movement on the official legislation front.

In his blog post titled “Still Not Dead: Why Legislators Should Kill the Online Streaming Act,” Canadian policy expert Dr. Winseck (2022) touched on the history of Bill C-11 by comparing it to Bill C-10, the Broadcasting Act reform bill. Winseck described Bill C-11 as not only failing to adopt significant changes compared to Bill C-10, but also being unsurprisingly subject to a “firestorm of criticism” for its consumer-type exemptions and free speech shortcomings, much like Bill C-10 (Winseck, 2022, para. 4). Winseck denotes the agreement in legal scholar Michael Geist’s article “Not Ready for Prime Time: Why Bill C-11 Leaves the Door Open to CRTC Regulation of User Generated Content,” who reminds Canadians that Bill C-11 failed to acknowledge individual users as broadcasters, a major error (Geist, 2022, para.3). To identify citizens as both producers and consumers would change the legislation in its entirety, and this is discussed in a later section of this MRP. Thus, the gap in legislative modernity still exists in Canada. The emergence of Bill C-11 in 2020 introduced the new CPPA which replaced part one of the current Personal Information Electronic Documents Act. It also introduced Bill C-27, the Personal Information and Data Protection Tribunal Act which established an administrative tribunal that will assess and levy penalties under new privacy law (Jacksch, 2021). According to section 4 of Bill C-11, the tribunal will have the duty of analyzing OPC decisions and ensuring compliance with the Bill (Government of Canada, 2022).

A few months following the release of Bill C-11 in the Fall of 2020, at the request of the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI), the previous Canadian Privacy Commissioner Daniel Therrien compiled and shared 60 recommendations for Bill C-11. The suggestions were split into two

annexes: Annex A and Annex B, and they addressed concerns regarding the issues the Bill did not adequately cover. Within the list of suggestions, Therrien explained that Bill C-11 "is frequently misaligned and less protective than the laws of other jurisdictions" (Government of Canada, 2021, para. 2). Therrien specifically pointed to many sections of the Bill that need revision (e.g., sections 5, 12, 13, and 44 to 50). The reason his list of recommendations is so notable is, as I will demonstrate, because certain recommendations (specifically 7, 8, 11 & 15) indirectly address dismantling the structure of digital colonialism (Therrien, 2021). In the early days of the Bill prior to the election call, Therrien's recommendations seemed to be shared by various bi-partisan politicians, and I, too, believe the recommendations have merit. Although it was difficult, I have selected four recommendations that unpack the significance of digital colonialism, which I will demonstrate in the subsequent section.

## Approach

The relationship between political economy and critical discourse analysis has been developed by academics Mulderrig, Montessori and Farrell (2019) in their work titled: "Introducing Critical Policy Discourse Analysis." Mulderrig et al. (2019) believe that two methods, critical discourse analysis and policy analysis, working in tandem have a three-fold benefit to research methodology and projects like mine that operate within a political-theoretical intersection. They argue that critical policy discourse analysis is a

> framework for conducting systematic, yet contextually sensitive, analysis of texts based on a critically grounded theory of discourse. Its abductive, multi-layered research methodology involves continual movement between theory, method, and data, allowing the researcher to link macro-social processes to micro discursive events such as texts or conversations. Second, it shares with CPS a number of

> important assumptions about the object of research, as well as epistemological, ontological, and normative principles, which in turn have implications for how research can and should be conducted. (p. 5).

As such, Mulderrig et al., (2019) hope that critical policy discourse analysis "makes a significant and highly practical contribution to the field of critical and interpretive policy studies" (p. 5).

In simpler terms, the authors devised a theoretical framework for research that is premised on the analysis of macro and micro texts. In succession, I will draw links between the macro-social processes of digital colonialism to the "micro-discursive" text that the previous OPC put forth in his Bill C-11 recommendations: 7, 8, 11 and 15. I deem critical policy discourse analysis the most suitable research method to use for my MRP because Bill C-11 is not only a proposed policy, but a policy that has faced heavy critique and has, thus, been the subject of plenty of discourse by the public, the experts, the government, and the previous Office of the Privacy Commissioner alike.

Therrien's recommendations are informed by a policy analysis lens. While the Office of the Privacy Commissioner has a general stance on policy reform written in the annual reports of 2019 and 2020, Therrien states that their Bill C-11 recommendations are spurred by the goal of upholding the importance of consumer consent and consumer's right to privacy by innovative legislation. Therrien's report states that, "At a minimum, the law should provide objective standards, democratically adopted in the public interest, that assure[s] consumers that their participation in the digital world will no longer depend on their 'consent' to practices imposed unilaterally by the private sector" (Therrien, 2021, para. 59). Consent is a highly analyzed term in Colonial and digital colonial literature.

Therefore, I decided to use Therrien's suggestions because they were well-informed, innovative, and generally well-received in the House of Commons (Government of Canada, 2021). Furthermore, it is the first official critical document of Bill C-11 that was not only requested by the Government but was put forth after hearing the discursive criticism from academics and experts alike, deeming it discourse-informed.

Is there validity in Griziotti's (2018) statement that "the hierarchy of governance no longer requires unconditional collective and explicit accessions, but rather applies a *laissez-faire* attitude on an individual level" (p.183)? According to Therrien on Bill C-11, yes. By analyzing why Therrien suggests Bill C-11 took a laissez-faire attitude as opposed to a human rights-based approach, Griziotti is correct in believing governments have not, at times, done enough to solve issues pertaining to techno-political intersections, thus leaving the responsibility on the citizens to demand change. Digital First Canada, an advocacy group for digital creators, has a current objective to fix Bill C-11, describing one major myth of Bill C-11 as a representation of being "fair, flexible and modern" when it is none of those things (Digital First Canada, 2022).

## Defining Digital Colonialism

In order to tackle this paper's objectives, which is to examine four of Therrien's Bill C-11 recommendations under a digital colonial framework, digital colonialism itself must be extensively defined. Because there are various definitions of digital colonialism, in this paper, I explore several explorations of digital colonialism from several authors (mainly Couldry and Mejias, 2019; Coleman, 2019; Griziotti, 2018; Mann and Daly, 2018; Mouton and Burns; 2021; Young, 2019; Pinto, 2021), in an attempt to draw out the themes addressed by Therrien in the following section.

While the subsequent sections of this paper will delve into specific definitions from various authors, I, first cite Wikipedia (2021) because it provides a valuable preliminary overview in layperson's terms. Comprehending the simplistic definition of digital colonialism is crucial for establishing an understanding of a complex framework like digital colonialism:

> Electronic colonialism or digital colonialism, sometimes abbreviated to eColonialism, was conceived by Herbert Shiller as documented in his 1976 text *Communication and Cultural Domination*. In this work, Shiller postulated the advent of a kind of technological colonialism, a system that subjugates Third World and impoverished nations to the will of world powers such as the United States, Japan, and Germany, given the necessary "importation of communication equipment and foreign-produced software." As scholarship on this phenomenon has evolved, it has come to describe a scenario in which it has become normal for people to be exploited through data and other forms of technology. It draws parallels to colonialism in the traditional sense when territories and resources were appropriated by the wealthy and powerful for profit. (Electronic Colonialism, 2021)

In summation, the Wikipedia definition of electronic colonialism describes it as the name for data exploitation that privileges the wealth holders through the exploitation of the colonized. Eight of the authors cited in the Wikipedia definitions (Couldry, Mejias, Coleman; Kwet, Young; Cohen; Mouton and Burns) are authors that will be referenced in this MRP.

Before I apply digital colonialism to Bill C-11, I will explore the arguments of relevant theorists who studied and explored the concepts. I chose these specific authors

because they each offer different approaches to digital colonialism, capturing perspectives from different continents and thought processes. Nevertheless, the authors exploring several aspects of digital colonialism that will be covered in the next section all share essential elements of the Wikipedia definition. Because I continued to identify identical concepts across all authors, I have chosen to group "data colonialism," "the new frontier," "electronic colonialism" and "digital colonialism" in the same category under digital colonialism. Because just as there is no single definition, there is no single term for digital colonialism, either; therefore, authors are free to call it what they wish. What is most important is the similarities and consistencies in the elements, themes, and subject matter. Similar to Colonialism, the authors agree that the best way to dismantle the digital colonial system is through digital decolonization; however, in order to address critiquing digital colonialism, it is important that we first understand what it is.

## Digital Colonialism: a Definition

Digital colonialism is a highly intricate, discursive theoretical framework. While I acknowledge the nuances present under the term 'digital colonialism,' the major conceptual takeaways fall under extraction, exploitation, and dispossession,[5] all of which will be addressed in this paper. Some categories include the use of sociality as commodity; the Scramble for African[6] data; the identification of the roles of the four

[5] When defining dispossession, "two critical conclusions can be drawn from these processes: First, accumulation by dispossession is an intrinsic process to capital that continues to occur in novel ways alongside other capital processes. In big data it continues its role as a key means by which capitalism staves off its inherent tendencies toward over-production. Second, it does so by corkscrewing into the body as well as the mind" (explained more on page 30) (Thatcher, 2016, p. 1000).

[6] "The Scramble for Africa (or the Race for Africa) was the proliferation of conflicting European claims to African territory during the New Imperialism period, between the 1880s and the start of World War I" (New World Encyclopedia, rev. 2023)

main actors of digital colonialism; the establishment of digital colonialism as a system of imbalance, power, and production; the exploration of digital colonialism in academia; the exploration of the dangers of data accumulation through dispossession; the exploration of the dangers of the logic of extraction; the nation-to-nation digital domination (in which the majority of the market consists of Western and Chinese platforms against little to no competition); the racial dimension of digital colonialism that bares similarities to the racial dimensions of Colonialism; the dismissal of Indigenous digital subjectivity; and the modernity of colonialism. I must use these core elements to consolidate a definition for this policy analysis. Without inventing my own definition but incorporating the stated explorations nonetheless, I believe digital colonialism is best defined by Couldry and Mejias' (2019) clear and concise explanation. According to them, digital colonialism is a "term for the extension of a global process of extraction that started under colonialism and continues through industrial capitalism, culminating in today's new form: instead of natural resources in labor, what is now being appropriated is human life through its conversion into data" (p. 19). Couldry and Mejias' definition will be the focus as I move onto the four highlighted recommendations by the previous Office of the Privacy Commissioner.

Additionally, it is crucial to mention that the application of Couldry and Mejias's term will follow the example of Pinto (2019), who not only focuses on what digital colonialism is, but focuses on how researchers can mitigate its harmful effects through decolonizing governmental policy. The following section loosely explores elements of the domains of digital colonialism (extraction, domination, and exploitation) and what these elements entail.

## The Four Actors of Digital Colonialism

Coleman (2019), when citing professors Hendricks, Marker, and Vestergaard from the University of Copenhagen, claims there are four rudimentary principal actors within digital colonialism. These actors are as follows:

1. *Technology corporations* from the West that collect and harvest data with the goal of improving their personalized ad targeting;
    a. In Bill C-11, these actors are referred to as organizations.
2. *Consultant and advertising businesses* that purchase the data from (1) to innovate and personalize their ad distribution with the purpose of profit;
    b. In Bill C-11, these actors are also referred to as organizations.
3. *The local parties and governmental organizations* who pay for this data (2) in order to spread their propaganda or simply aid the reputation of their respective countries; and
    c. In Bill C-11, these actors are referred to as organizations.
4. *The extractees: the citizens* who are either aware or unaware of the fact that they are data plains[7], ready to be harvested by the preceding actors (Coleman, 2019, p. 423).
    d. In Bill C-11, these actors are referred to as consumers.

## The Social Quantification Sector

Couldry and Mejias define "data colonialism" as the way in which human social interaction is now used for others' profit through various types of quantification, namely,

[7] I use the term 'data plains' to represent extractees as a response to Coleman's use of the phrase "data harvesting." The plains constitute the body in which data is harvested, similar to how plains are harvested for food in agriculture.

data relations. In this context, data relations are how corporations have commodified the way society interacts with digital information (data). In their book *The Cost of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism*, Couldry and Mejias (2019) explicitly define what they call data colonialism as a "term for the extension of a global process of extraction that started under colonialism and continues through industrial capitalism (Marx), culminating in today's new form: instead of natural resources in labor, what is now being appropriated is human life through its conversion into data" (p.22). They believe that data colonialism is operationalized through what they call "the social quantification sector," which is essentially a term for the notion that humans' social lives are the raw material for an entire industry.

Regarding colonizing social relations, Couldry and Mejias (2019) state that digital colonialism is an extension of the Marxist definition, in that: Data colonialism would be inherently unstable if it could not translate its methods alongside innovative social relations. As Dyer-Witheford (1999) pointed out in an early analysis of data and platforms, capitalism has always approached the internet as a domain in which control over the communicative capacity of individuals would allow capital to appropriate not just labor but also, as Marx himself put it, labour's "network of social relations" (p.12).

According to Couldry, Mejias, and Marx – Colonialism and capitalism are historically and economically linked.

However, as digital colonialism is an extension of Colonialism, Couldry and Mejias adopt the term "data relations" to explain the normalization of the appropriation of personal data. It is normalized through its ubiquity in that, "Through data relations, human life is not only annexed to capitalism but also becomes subject to continuous

monitoring and surveillance. The result is to undermine the autonomy of human life in a fundamental way that threatens the very basis of freedom, which is exactly the value that advocates of capitalism extol" (Couldry & Mejias, 2019, p.14). Under data colonialism, how people socialize is revealed as one of the most economically profitable and, thus, sought out areas of life by corporations, governments, and citizens seeking employment. For instance, in 2013, *The Entrepreneur* reported that digital marketing careers have skyrocketed because companies understand the profitable endeavor that is capitalizing user's time spent on social media:

> Ten years ago, calling yourself a "social media manager" would likely have been met with a confused look and the assumption that you waste your time goofing off on Facebook. But over the last few years, careers in social media have exploded as companies realize the value of reaching their customers on the medium where they spend most of their time. According to data from LinkedIn compiled by social marketing platform Offerpop, there has been a remarkable 1,357 percent increase in social media positions posted on LinkedIn since 2010 (Davis, 2013, para.1).

The social quantification sector has a significant effect on the labour market because data relations are not free from commodification, bidding, and pricing. In fact, the opposite is arguably true, as economics under Couldry and Mejias's data colonialism revolve around the exploitative quantification of social relations on social media platforms (Couldry & Mejias, 2019, p. 22). For instance, 'Idle no More,' a 'Canadian' Indigenous-led social movement campaign that supports Indigenous sovereignty, gained a massive amount of support on various social media platforms. However, the real success of the Idle No More campaign was seen by the large data companies that

accumulated the data of the campaign supporters and sold them to advertisers (Couldry & Mejias, 2019, p.8). On the topic of the movement, Leanne Betasamosake Simpson, a supporter of the movement, an academic and artists of the Nishnaabeg people, said

> every tweet, Facebook post, blog post, Instagram photo, YouTube video, and email we sent during Idle No More made the largest corporations in the world more money to reinforce the system of settler colonialism. I wonder in hindsight if maybe we didn't build a movement, but rather we built a social media presence that privileged individuals over community, virtual validation over empathy, leadership without accountability and responsibility. (Simpson in Couldry & Mejias, 2019, p. 82)

In *Raw Data is an Oxymoron* (2013), a series of essays compiled by Lisa Gitelman, she explains how data is not, in and of itself, raw. The nuances around raw data can be strategically presented as something it is not, depending on who is the narrator. Specifically pertaining to the way it is consumed, used, and exploited, Garvey's essay about how newspaper articles were used to track runaway slaves in the South is an example that proves that unjust data collection may be presented as something just (i.e: reprimand the slaves for the betterment of society), even if the outcome is anything but just (i.e: locate the slaves, so that we can enslave and torture them further) depending on who is controlling the narrative (Garvey, 2013, p. 10). In Bailey's (2013) essay, Bailey, too, argues that the surveillance of data (or dataveillance) can be, and has been, weaponized, leaving the data extractors more powerful, while leaving those who had their data extracted falling into a state of helplessness. Both essays assert that the data is not raw, due to the "transformation of human life into raw material resonating strongly with

the history of exploitation that preceded industrial capitalism—that is, colonialism" (Couldry & Mejias, 2019, p.22).

One way to understand how data reflects inequality under digital colonialism is by exposing the pattern of nuanced language in extractive digital contracts. Under Colonialism, ambiguous agreements were used to protect the colonizers and manipulate the colonized to sign (Gitelman, 2013). To understand the social power of data is to understand its legislators, its programmers, its sellers, its extractors, its producers, and its strategically nuanced terminology. In *Algorithms of Oppression*, Noble (2018) argues that "at present, Google's search engine promotes structural inequality through multiple examples and that this is not just a design problem but an inherent political problem that has shaped the entirety of twentieth-century technology design" (The International Journal of Information, Diversity, & Inclusion in Noble, para. 15).

Couldry and Mejias' (2019) definition, on the other hand, distinguishes their definition from the other definitions that involve unwarranted settlement over an Indigenous population because data colonization "is not an approximation of other experiences of oppression but a highly distinctive exercise of power" (p.11). To Couldry and Mejias, this distinctive exercise of power is typified by Indigenous dispossession, cultural invasion, and appropriation, which are themes that will be explored in the following section. While Colonialism had an extractive focus on various resources that would give colonizers economic, political, and social might such as oil; data colonialism only has data.

Couldry and Mejias argue that the current state of data colonialism is beneficial to data colonizers (governments, corporations, or organizations) because buying and selling

data is a lucrative business and colonizers are the sole bodies with the means to buy and sell it (2019). They reference IBM's company statement that says, "Just as large financial marketplaces create liquidity in securities, currencies and cash, the IoT can liquify whole industries, squeezing greater productivity and profitability out of them than anyone ever imagined possible" (p.24). IBM states this with an air of positivity, because the company owners acknowledge that they have a monopoly over the data market. IBM's boastfulness demonstrates just how unconcerned they are about losing control of that monopoly. Monopolies over data ownership are beneficial for companies and corporations only. However, in order for this imbalanced relationship to work, "every layer of human life, whether on social media platforms or not, must become a resource from which economic value can be extracted and profit generated" (IBM in Couldry & Mejias, 2019, p. 23).

The problem with this is that, in order to extract and profit from data, one would have to be in a position of power (such as a company, governments or a corporation) to extract and profit from the buying and selling of data. Unfortunately, as it stands regular consumers cannot extract data and sell it for profit. Today, there are only two bodies able to do that: corporations and governments. Couldry and Mejias argue that

> humanity's "everyday relationships with capital are becoming colonial in nature," and the only way to understand them is by seeing them as an appropriation of capitalism (2019, p.12). By becoming colonial in nature, Couldry and Mejias are referring to the systems of domination that supported the extractive policies developed by Western Colonial powers after 1492, including the decimation of Indigenous civilizations and the widescale use of slave labor (2019, p. 69 & 83).

The critical analytic dimension of data colonialism as a conceptual framework, to Couldry and Mejias, is rooted in the Marxist critique of capitalism, specifically in the exploitation of human labour. Marx maintained a core acknowledgment of capitalism's toxic, expansionary potential and, even so, Couldry and Mejias (2019) believe Marx could not have predicted what has come of Colonialism, due to its ubiquity and widely accepted impact on society (p. 5). However, in the section of their book titled *Updating Marx for the Age of Big Data* Couldry and Mejias distinguish their stance because they do not feel their argument is in accordance with orthodox Marxism. Rather, they claim it is an extension of it. Data colonialism is not entirely new; it is both a culmination and a continuation of colonialism by other means, as opposed to a lapse or outlier in the historical arc of Colonialism (2019). On the topic of why they regard it as a Marxist-term, they write:

> If, following Marx, we understand capital not as static accumulations of value and resource but as "value in motion," then the appropriation of data enables new ways of forming capital through the circulation in trading of informational traces (data). But the trading of data is only part of a larger change whereby capital comes to relate to the whole world, including the world of human experience, as an extractive resource (Couldry & Mejias, 2019, p. 34; Harvey, 1996, p. 63).

The current advantage for colonizers under digital colonialism lies in the normalization of extractive resources. When Colonialism seized up, it was because the oppressed fought back against the system. The colonized utilized decolonial regimes, which are processes that dismantle the unbalanced systems of Colonialism. By feeding

into the notion that data extraction is acceptable, we are giving it power. Couldry and Mejias "are not arguing that data colonialism represents a new, fully formed mode of production. Rather, we are proposing that data colonialism represents a transformation that will eventually result in a new mode of production" (2019, p.86). This revolutionized the economic Colonial mode of production with its lasting adverse effects in the social quantification sector. From their perspective, in general the threat of data colonialism is that "it undermines the autonomy of human life in a fundamental way that threatens the very basis of freedom" (Couldry & Mejias, 2019, p.14). If the threat of digital colonialism is indeed real, then it is essential to observe a bill as crucial as Bill C-11 through both a colonial and decolonial lens, ensuring that rights and freedoms[8] such as equality remain intact.

One purpose of this paper is to explore Bill C-11 and its deserved or undeserved negative reception through the lens of digital colonialism. Mouton and Burns (2021) postulate that, as a researcher, the desire behind wanting to research digital colonialism is a direct result of the fact that, "as the 'datafication' of our daily lives progresses and attracts mounting attention in academic realms, scholars find themselves in need of new conceptual tools to make sense of the latest developments in data-intensive forms of capitalism" (p. 1892). It is imperative to highlight that many academics such as Couldry and Mejias (2019), Kwet (2019), Mann and Daly (2019), Stingl (2015), Thatcher et al., (2016), and Young (2019) agree that "in recent years, the concepts of 'digital colonialism' and 'data colonialism' have gained considerable currency," which [they] postulate is because data is being regulated as a profitable resource (Mouton & Burns,

[8] Canada's Charter of Rights and Freedoms (1982) protects a variety of arguments noted in digital colonialism, such as equality rights and citizen's protection against unreasonable laws.

2021, p. 1892). Such momentum is primarily where aspects such as extraction, dispossession, commodification, and exploitation exist. Academics acknowledge that digital colonial scholarly research has not yet stabilized; therefore, researchers attempt to establish it to the best of their ability.

## The Logic of Extraction

The logic of extraction, in the case of digital extraction, is the acknowledgment of online information used, treated, and regarded as a resource. In the context of my analysis, the logic of extraction stems from the Colonial logic of extraction, in which Colonial powers stole the regions they controlled. It was said, from a colonizer's perspective, that "the ideological justification for the dispossession of Aborigines was that "we" could use the land better than they could, not that we had been on the land primordially and were merely returning home," exposing dispossession as the opposite of a human rights-based endeavour (Wolfe, 2006, p. 389). Even further, the logic of extraction can be regarded most simply, as one-sided basic trade: in which one actor takes something from another actor because it benefits the traders economically[9]. Much like oil extraction, it is not extracted for no reason; therefore, in the context of digital colonialism, the inherent logic behind the cause of extraction is the imbalanced benefit it brings the organization doing the extracting.

## The New Colonial Apparatus

[9] In Lewis Mumford's "Technics and Civilization," Mumford explains how hunters created the first valuable invention, because hunters extracted for their own use: food (1934). What's more, Mumford (1934) states that the rulers of Europe were hunters and fishers because they essentially mastered the art of extraction, in that they understood the objective of hunting is to conquer man. It is not enough to simply trade, one who trades must get more out of the trade than the other constituent. Because of this, an unfair transaction is a good transaction. For the past rulers, destruction was more important than the origin (Mumford, 1934).

Srnicek (2016) states that there are five types of platforms that dominate the current digital infrastructure: advertising platforms, cloud platforms, industrial platforms, product platforms, and lean platforms. Srnicek states that all five platforms were initiated by capitalistic crises, such as the 2008 economic crash, and exist and are successful today due to their reliance on extracting digital content and personal data from users. Srnicek states that platforms, as powerful as they are now, are only powerful in that they can extract data. In fact, Srnicek calls platforms "an extractive apparatus for data." Platforms mirror the behavior of Colonizers because

> By providing a digital space for others to interact in, platforms position themselves so as to extract data from natural processes (weather conditions, crop cycles, etc. from production processes (assembly lines, continuous flow manufacturing, etc.), and from other businesses and users (web tracking, usage data, etc.)." (p. 48)

Data extraction is the center of platforms' business models. Platforms cannot exist without this extractive relationship of free labour; therefore, Bill C-11 should be questioned in respect to its platform regulation (Srnicek, 2016, p. 53).

## A Shipment of Codes

Mouton and Burns (2021) exemplify the consistency of thinking across digital colonial theorists by citing Couldry and Mejias' exploration of two different strands of literature pertaining to digital colonialism, while choosing to use the same term that Grizzioti (2018) uses with the 'New Frontier.' Mouton and Burns identify the first strand of digital colonialism as the discovery of a 'digital realm' in a new continent, a new frontier waiting to be explored and exploited, while tech companies could be viewed as

the modern version of Colonial caravels. Nonprofit organizations, such as ICANN, exploit data just like the Spanish and Portuguese exploited the colonies they colonized: without permission, and for the benefit of their country and the detriment of the other" (Mouton & Burns, 2021, p. 1894).

The governmental body that sent these caravels, giving settlers the right to do the deplorable things they did when conquering other countries was instructed by governments or active rulers. Therefore, the metaphorical conceptualization of data extractors representing caravels exposes not only the selfish role of the tech companies, but their close relationship with legislative bodies that enable their potentially questionable behaviour. At this point, it is important to establish that what all the authors I have explored so far have in common is their call for citizens to beware of their powerful, multi-faceted data extractors.

**Submission of the Office of the Privacy Commissioner of Canada on Bill C-11**

In the beginning of his document of suggestions to improve Bill C-11, the previous Privacy Commissioner Daniel Therrien stated that Bill C-11 has potential to improve the Consumer Protection Act; however; it is lacking where human rights are concerned.

Following the research of Dr. Scassa, the Canadian Research Chair in Information Law and Policy, Therrien concluded that Bill C-11 needs to apply a human-rights-based approach to this area of legislation. He contends that Bill C-11 is a step back for Canadian privacy protection; thus, I postulate that applying a digital colonial lens to Bill C-11 amendments could be a useful subsequent step to a human rights-based Consumer Protection Act. Therrien acknowledges that there is a decrease in trust in data protection

during the digital revolution and, to mitigate the distrust, "The regulation required is sensible legislation that allows responsible innovation that serves the public interest and is likely to foster trust, but that prohibits using technology in ways that are incompatible with our rights and values" (Therrien, 2021, para. 11). There is nothing more compatible with Canadians rights and values[10] than the avoidance or dismantling of colonial structures[11].

Following Therrien's proposal for Bill C-11, my recommendation is that the OPC utilizes digital colonialism as a lens to identify ways Bill C-11 can put human rights and decoloniality at its forefront. Therrien (2021) states that "Parliamentarians now have a chance to confirm or amend this direction" and "There is no dispute that the CPPA should both promote rights and commercial interests. The question is what weight to give to each because when there is a conflict between the commercial interests and interests of the citizens, human rights should undoubtedly prevail" (para. 21). According to Canada's OPC, a human rights-based approach to Bill C-11 is mandatory. And the way the government can give weight to rights and commercial interests is to ensure that Indigenous subjectivity, and, by extension, digital decoloniality, is a lens applied to this proposed legislation.

While Bill C-11 is predominately focused on the privacy of individuals, and digital colonialism is more of an analytic framework, applying a digital colonial lens to Bill C-11 can reveal the areas that could be improved for Indigenous communities. In

[10] In addition to the Canadian Charter of Rights and Freedoms, Canadian values include valuing the rights of Indigenous peoples, and the protection of cultures and traditions from other parts of the world within Canada, known as multiculturalism (Canadian Charter of Rights and Freedoms, 1982).
[11] And as a reminder: the Canadian Government, referencing Duarte, also stressed the importance of Indigenous self-governance is in "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians" (2018).

fact, when Therrien (2021) explains that consent is arbitrary and that “simply put, it is neither realistic nor reasonable to ask individuals to consent to all possible uses of their data in today’s complex information economy [because] the power dynamic is too uneven” it is possible that he was indirectly referencing the power imbalance between consumers (actor 4 according to Coleman) and Big Tech companies (actor 1 according to Coleman), also known as the controllers of data established by every single author explored in the definition section. Both actors 1 and 4 (the big tech companies and its consumers) are addressed in the recommendation document. This differs not from what the digital colonial researchers argued when they contrasted the colonizers and the colonized. Such a connection is important when bridging the gap between policy and theoretical frameworks. Furthermore,

> Thatcher et al. (2016) “have called for the development of a political economy of data, to better understand the role of the digital in everyday processes of capitalist exploitation … in each case the researchers call for greater attention to the colonial implications of technology engagement.” They even mobilize the theory of 'accumulation by dispossession' in order to explain why and how data is extracted from its producers to increase revenue for its extractors (Young, 2019, p. 1425).

Considering what I have gathered about the basis of digital colonialism thus far, I will now highlight four of Therrien's recommendations that addressed the major concerns of digital colonialism such as extraction, domination, and labour exploitation. I will do this by presenting each selected recommendation. Then, I will explain why these particular recommendations address digital colonialism and digital decoloniality. The

four recommendations directly pulled from the previous OPC Daniel Therrien to amend Bill C-11 are as follows, followed by each of its connections to digital colonialism and decoloniality.

Building on my discussion of digital colonialism, I will now apply its theoretical framework to a specific governmental document, Therrien's recommendations. Using Couldry and Mejias' definition of digital colonialism, I will unpack the significance of these recommendations while using elements of critical discourse policy analysis. Griziotti (2018) believes that once we establish the root cause of digital policy issues, the following step is called "do-ocracy," which is the demand for democratic practices rooted in individual action. The subsequent section of this major research paper is my do-ocracy, in that I will act by uncovering potential answers to Bill C-11's issues and my research questions *(What is digital colonialism and how, from a digital colonial standpoint, can we unpack recommended amendments 7, 8, 11 and 15 proposed by the previous Office of the Privacy Commissioner)?* What I have discovered is that one of the solutions that can be used to improve Bill C-11 is digital decoloniality; therefore, applying a digital colonial analytic framework to these recommendations will be my first step in the direction of improving the Consumer Privacy Protection Act.[12]

[12] **Disclaimer:** the following highlighted recommendations are only four of sixty. I have selected these four because they best address the elements of digital colonialism. However, my stance on the matter is subjective. Further analysis outside the confines of my MRP remains needed.

**Recommendation 7:**

Definition of personal information

As discussed in the OPC's recent publication, A Regulatory Framework for AI: Recommendations for PIPEDA Reform (AI paper) and elaborated in the accompanying paper from Professor Ignacio Cofone, an important measure related to the human-rights approach would be to amend the definition of personal information so that it explicitly includes inferences drawn about individuals.

Inferences refer to a conclusion that is formed about an individual based on evidence and reasoning. In the age of AI and big data, inferences can lead to a depth of revelations, such as those relating to political affinity, interests, financial class, race, etc. This is important because the misuse of such information can lead to harms to individuals and groups in the same way as collected information – a position confirmed by the Supreme Court in Ewert v. Canada. In fact, as noted by the former European Article 29 Data Protection Working Party, "[m]ore often than not, it is not the information collected in itself that is sensitive, but rather the inferences that are drawn from it and the way in which those inferences are drawn, that could give cause for concern."

General support for the idea that inferences constitute personal information can be found in past OPC decisions and Canadian jurisprudence. For instance, the OPC has found that credit scores amount to personal information (2013 PIPEDA Report of Findings, among others), and that inferences amount to personal information under the Privacy Act (2015 Accidental disclosure by Health Canada, paragraph 46). This is also consistent with the Supreme Court's understanding of informational privacy, which includes inferences and assumptions drawn from information.

However, despite this, there remains some debate as to how inferences are regarded. Some view them as an output derived from personal information, much like a decision or an opinion, and argue these are outside the purview of privacy legislation. Given that inferences are typically drawn using an analytical process, such as through algorithms, others claim that these are products created by organizations using their own estimations, and that they do not belong to individuals.

In light of these conflicting viewpoints, we believe the law should be clarified to include explicit reference to inferences under the definition of personal information.

This would be in accordance with modern privacy legislation such as the California Consumer Privacy Act (CCPA), which explicitly includes inferences in its definition of personal information. The OAIC's proposed ammendments to the Australian Privacy Act also support this approach.

Importantly, even where there is agreement that inferences are personal information, the fact that they could reveal commercial trade secrets is used by some as a basis to deny individuals certain privacy rights, such as to access or correction. Our recommendations for automated decision-making propose a fair way to resolve this contention.

---

*Source:* Daniel Therrien, Submission of the Office of the Privacy Commissioner of Canada on Bill C-11 the Digital Charter Implementation Act, 11 May 2021.

Recommendation 7 indirectly acknowledges the potential detriment caused by the imbalanced contract of data collection. That detrimental factor is inferences. To infer that data is free for the taking is to do as Colonizers did. To use nuanced jargon in the unfair contracts is to do as Colonizers did. The third and fourth actors from the four actors of digital colonialism section explain the motives and interests for the policy analysis component of this research paper. If adopting Coleman's four categories from page 14, in which actor 1 (1) refers to tech corporations, actor 2 (2) refers to advertising companies, actor 3 (3) refers to governments, and actor 4 (4) refers to extractees, then the acts of the Government of Canada (3) in legislating data for Canadian citizens (4) implies that governments may have an alternative agenda for data relations that are profit-driven and not driven by the citizen's well-being per se. But can the government be driven by both? The history of Colonialism disproves this ethical theory. The acts of governments and citizens both point to the idea that citizens may or may not be knowledgeable enough about digital colonialism, which leaves them vulnerable during data extraction which reveals personal information. That personal information is inferred upon extraction, which could be dangerous according to Therrien. Despite Coleman focusing on the West-into-Africa case study, the analysis of digital colonialism can also apply to the Canadian example. Coleman (2019) cites scholar Kwet (2019) who believes that Western tech companies

> Design digital technology to ensure their own dominance over critical functions in the tech ecosystem … this allows them to accumulate profits from revenues derived from rent (in the form of intellectual property or access to infrastructure)

> and surveillance (in the form of Big Data). It also empowers them to exercise control over the flow of information (such as the distribution of news and streaming services), social activities (like social networking and cultural exchange) and a plethora of other political, social and economic and military functions mediated by their technologies (p. 8).

The benefits that Western technology companies receive as a result of digital colonialism go a long way in validating the existence of digital colonialism. Colonizers, both digital and historical, benefit from a system of extracted and inferred information; therefore, digital colonizers are rewarded for upholding that system. Therrien's 7th recommendation explicitly asking Bill C-11 to reference the dangers of inferences in the CPPA's definition of personal information is a crucial element to digital decolonial thinking because to admit that "in the age of AI and big data, inferences can lead to a depth of revelations, such as those relating to political affinity, interests, financial class, race, etc." is an acknowledgement of the potential dangers of data handling under an unbalanced system (Therrien, 2021, para. 3). If personal information is extracted from actor 4 by actors 1, 2 and 3 then inferred by actors 1, 2 and 3, then it is no longer raw, creating dire consequences for actor 1, consumers (Gitelman, 2013).

## Consequences: Racial Dimensions

Where the lines between governments, tech corporations, and consumers remain blurred, Canadian academic Jason Young (2019) attempts to unblur the lines through critical race theory and research. Young acknowledges the unexplored aspects of digital colonialism in Canada by presenting the Indigenous perspective on digital colonialism, especially as it pertains to politics of epistemology and digital practices forced upon

Indigenous communities. Young demonstrates how Indigenous communities in the Canadian Arctic do not have equal access to digital technologies. For example, there are areas in the Canadian Arctic that have slower internet access comparable to the speeds of internet in the 1990s. As a result, the inhabitants of these communities cannot partake in the potential benefits of said technologies such as global, national, and local information on-demand. In Duarte's 2017 book *Network Sovereignty*, she explains how Indigenous communities in America strategically use their internet access to further their self-governance. Of course, the unequal access that Indigenous communities experience is due to the aftershocks of Colonialism, when Indigenous communities were stripped of their personal information before being purposefully ostracized, dispossessed, and forced to assimilate against their will (Young, 2019). The remnants of that ostracization, dispossession, and forced assimilation are present in the inferences of their data today.

The racial dimension of digital divide research has been explored by Ruha Benjamin (2019) in her book *Race After Technology*, where Benjamin argues that software often incorporates the biases and prejudices of the programmers themselves. The danger of information and communication technologies to people of colour is that the programmers who created these programs are often Eurocentric individuals who have not consulted Indigenous people, or other minorities for that matter, for their input on the technologies they are encouraged to use. This stimulates misunderstanding between electronics and people of colour, as it re-enforces the idea that Indigenous communities need an external, Euro-centric body to govern their lives and retrieve their information. In other words, "[t]he simplest explanation for biased algorithms is that the humans who create them have their own deeply entrenched biases. That means that despite perceptions

that algorithms are somehow neutral and uniquely objective, they can often reproduce and amplify existing prejudices" (Benjamin, 2019, p. 50).

Data collection algorithms, such as search engines, are not raw. They are riddled with inferences programmed by digital colonizers, but these colonizers will present it as an unbiased algorithm nonetheless. It is problematic that the "internet—long framed as a value-free tool for advancing human knowledge—frequently replicates the flawed societal power structures in which it was created, perpetuating stereotypes and racism under a guise of impartiality" (Algorithms of Oppression, 2021). For example, Canadian databases have been proven to overwhelmingly favour the discourse of white people while disfavouring the discourse of visible minorities (Noble, 2018). This algorithm is oppressive by nature, because boosting solely white voices goes against the supposed attempt to have ICTs reflect the actual Canadian demographic (Noble, 2018, p. 141). Furthermore, Benjamin (2019) exposed certain AI for establishing a Euro-centric beauty standard to compare pictures against (in which ethnic faces were deemed less attractive than their white counterparts by an "unbiased" AI bot. Benjamin then exposes the dangers of the same logic for more substantial political issues like police surveillance technologies that run on inferences (2019).

Regarding digital colonialism and predictive policing in Ottawa, Canada, the inferences embedded in these preemptive algorithms are said to be a cause for concern by Canadian lawyers such as Khoo who specializes in technology and human rights. Rudin, the program Director at Aboriginal Legal Services agrees with Khoo's caution that:

> While algorithmic policing technology may seem futuristic, it is inseparable from the past. The historical and ongoing patterns of systemic discrimination in

> Canada's criminal justice system are embedded in police data and related databases. Where this data is used to train algorithms ... the resulting algorithmic technologies will replicate, amplify, and exacerbate those discriminatory patterns. (in Canadian Press, 2020, para. 21)

The Privacy Director for the Canadian Civil Liberties Association (CCLA) also admits that these algorithms have the capacity to unintentionally discriminate against racial minorities.

For Young, in terms of Indigenous knowledge politics in Canada, there is still work to be done. He believes that research into ICTs "has not yet developed as nuanced of an approach to the epistemic biases of technology" because not enough Indigenous communities are being consulted for them (2019, p. 1426). Therefore, ICTs are run upon a system of inferences created by non-Indigenous groups. Through interviews, Young discovered that some Indigenous communities may find it difficult to trust ICTs the way other communities can, because in their culture, "people should not trust knowledge that does not come directly from someone that they know and trust, so that they are certain the information is valid" (Young, 2019, p. 1428). As we have seen under Colonialism, Indigenous communities are well justified in their wariness of Western governmental agendas. At the end of the 19$^{th}$ century, "Treaty 6 negotiations ended with promises of health care, education, hunting rights and freedom in exchange for sharing the land to the depth of a plough. However, instead, the Canadian government passed the Indian Act which forced Indigenous people onto reserves" where famine and abuse forced Colonialism and assimilation on the Indigenous communities (CBC, 2020, para. 2). If these communities should not trust all sources of information, then it only makes sense

that they should not trust actors, like governments (3), advertising agencies (2), and tech corporations (1) who want to profit from their inferred information for something the Indigenous communities were not consulted for. This betrayal is critical information[13] for both the government and the tech companies that handle their data, as the government is asking Indigenous communities to trust the same bodies that exploited their trust previously.

As a Yaqui information scientist, Duarte (2017) discovered that even the mere use of information technologies was used to resist the initial colonial view that regarded these communities as primitive. She contends that, for the Native peoples that she has studied across Indian Country in America, the use of ICTs not only contributes to their sovereignty and economic endeavours; it is also used in a manner that preserves their cultural heritage. In this respect, natives in the American Indian Country differ from other cultures that might not think of colonial resistance when using ICTs (Duarte, 2017). These reasons support Recommendation 7, which states that being cautious of inferences "is important because the misuse of such information can lead to harms to individuals and groups in the same way as collected information."

Young (2019) found that Indigenous peoples trust the elders in their community above all else. Presumed elder trust in Indigenous communities "is particularly the case today, given that elders are now often the only Inuit peoples that grew up largely outside of the colonial structures that shape Inuit life," so those who are forgetful of this fact

[13] **Implied Consent** is explicit permission that may not follow the valid consent guidelines of sec.15(1) of Bill C-11: the Consumer Privacy Protection Act but has still been established as valid by an organization. However, sec. 52(4) explicitly states that organizations do not have the right to rely on implied consent when collecting personal information described in paragraph (2)(a), (2)(b),(3)(a), or (3)(b) (Government of Canada, 2020).

(mainly the current Indigenous youth) are seen as ignorant and disrespectful to their culture (p.1428). Furthermore, through his interviews Young found that Indigenous communities of the Canadian Arctic, Young inquired about digital technologies and colonialism as separate entities, and their experience largely supported the argument that the dismissal of digital colonialism is altering the maintenance of their culture. Young is clear that Indigenous cultural maintenance "is a relational, subjective, private, and personalized model of knowledge transmission, in contrast to knowledge systems in Western science that emphasizes objectivity, separations between knower and knowledge, and certification of authority through a colonial education system." (Young, 2019). Nevertheless, Indigenous communities are treated as a Canadian monolith in Bill C-11 despite the fact that Indigenous knowledge differs from Canadian ones. It differs in that Indigenous knowledge emphasizes emotional subjectivity, and mutual respect between the elders and the information they share, without the certification from an exterior colonial education that oppressed them. Indigenous Subjectivity is crucial to the longevity of knowledge systems in Indigenous communities. In this respect, the idea that data collection is inherently at odds with Indigenous knowledge systems is why the OPC is calling for an amendment of the definition 'personal information' to include the potential of dangerous inferences.

Furthermore, contrary to the regulation in Bill C-11 that does not include the dangers of inferences in its definition of personal information, the only people who should be judging the information of Indigenous communities are Indigenous communities themselves. Valid Indigenous self-governance is the practice of Indigenous subjectivity and decoloniality. Therefore, the very data the actors 1, 2, and 3 extract from

actor 4, such as their "credit scores," are judged against Western standards of analysis that the Indigenous communities did not agree to nor subscribe. Ruha Benjamin (2019) has already established that algorithms can be racist, and increased surveillance presents a danger to racial minorities. In this recommendation, Therrien stated that some people consider algorithms to be something that does not belong to the individual; an implication that there is an issue with ownership and data. It also implies that there is a difference between different actors, because if algorithms do not belong to the individual (actor 4) then they may unfairly belong to those who develop the algorithms (actor 1, 2 & 3). This could be regarded as an admission of the power imbalance between tech corporations and consumers. All the authors I have explored in my literature review so far called for citizens to be aware of their data extractors because of the power imbalance. They did not warn citizens against biting the hand that feeds them. In fact, they support decolonial regimes (Couldry & Mejias; 2019, Pinto, 2021). Therefore, Therrien suggesting that inferred information be clarified, explicitly defined, and regarded as sensitive information is a step in the right direction.

Organizations such as Big Tech companies claim that this type of clarification can infringe on their privacy rights, but these claims are not strong enough to dismiss the speculation of inferred information. An organization's concern that their trade secrets will be disclosed in a government required attempt to be more transparent with consumers is a privilege to privacy not granted to consumers. Organizations want users to forfeit their right to their private information in order to generate profit. These organizations then ask those same users to respect the organization's refusal to disclose for what purpose they

are selling consumer information, a luxury not granted to Canadian citizens or Indigenous communities.

Finally, defining personal information and including the clarification of inferences is not a new endeavour. In the 7th recommendation Therrien alluded to Australia, a place which has long been characterized by its colonialism, having already amended their Consumer Privacy Protection Act to state that the definition of personal information be amended to expressly include inferred information. This, once again, proves that Canada is a step behind the rest of the world (Mann & Daly, 2018).

## A System of Imbalance, Power, and Production

In their article titled "(Big) Data and the North-in-South: Australia's Informational Imperialism and Digital Colonialism," authors Mann and Daly (2018) demonstrate why Recommendation 7 was inspired by the example of Australia. They used digital colonialism to understand the Australian case study as a unique Western nation in the Global South. Many of the points they make supported the stance of Kwet, in which it should be highlighted that they define digital colonialism relative to Colonialism, because while they find that "traditional colonialism represents the physical presence of a colonial power in a given geographical place, predigital data gathering about colonized peoples and its use, including through categorization as a means of colonial control, is not new and has characterized colonial and postcolonial countries including Australia for some time" (Mann & Daly, 2018, p. 381). In effect, similar to the thoughts of Couldry and Mejias (2019), digital colonialism to Mann and Daly is a continuation of Colonialism in terms of its imbalanced handling of power and production (where the Colonizers exploited the Colonized). In the decolonial Australian explanation of digital colonialism,

Mann and Daly operationalize Connell's "Southern Theory[14]" to gather several formative examples that form an Australian case study in which:

> interesting attention is focused on the power relations between the Global North and Global South—that is, the systems of academic inquiry and thought, and geopolitical, economic, and legal interactions that preference, and place at the top of the hierarchy, a Northern/Western, largely Anglophone, worldview—at the expense of Southern alternatives. (Mann & Daly, 2018, p. 381)

Mann and Daly (2018) believe that the dismissal of alternatives from the Global South is in accordance with Colonialism, in which some of those Southern alternatives "include local, Indigenous, and ethnically diverse perspectives, underpinned by "resistance, subversion, and creativity" among the voices of those often lost within Northern/Western dialogue" (p. 380). However, where Mann and Daly focus predominately on the racist and oppressive elements of digital colonialism from a national and transnational perspective (suffered, at large, by Indigenous populations in Australia), Couldry and Mejias (2019) take a broader stance by exploring how data colonialism impacts Indigenous populations as well as anyone who contributes to the social quantification sector at large. For instance, Couldry and Mejias mention how "The mission statements of social quantification companies do not mention anything about extermination of natives" in that the governments did not acknowledge the enslavement of the colonized in the legislation (p. 106). The Australian example has been referenced by Therrien in Recommendation 7 because he believes Bill C-11 needs a human rights-based framework similar to the *Australian Privacy Act*. In the preface of the Canadian

[14] Raewyn Connell define "Southern Theory" as the the use for social thought *from* the societies of the global South. It's not necessarily *about* the global South, though it often is" (Connell, 2010).

OPC's Bill C-11 recommendation document, Therrien (2021) cites the Office of the Australian Privacy Commissioner, who stated:

> However, balancing privacy rights with economic, security and other important public interest objectives is not a zero-sum game. There are mutual benefits to individuals and regulated entities if the rights and responsibilities in the [Australian] *Privacy Act* are in the correct proportion. Effective privacy laws support economic growth by building trust and confidence that innovative uses of data are occurring within a framework that promotes accountability and sustainable data handling practices. Increasing individuals 'confidence in the way their personal information is managed will likely lead to greater support for services and initiatives that propose to handle this information. These are essential ingredients to a vibrant digital economy and digital government.

**Recommendation 8:** That a definition of sensitive information be included in the CPPA, that would establish a general principle for sensitivity followed by an open-ended list of examples.

Definition of sensitive information

Under subsection 12(2)(a), one of the factors to consider when determining whether a reasonable person would consider an organization's purposes appropriate under the circumstances is "the sensitivity of the information." This is also a consideration that organizations must take into account with respect to the form of consent (s. 15(4)), the development of an organization's privacy management program (s. 9(2)), the level of protection provided by security safeguards (s. 57(1)), the evaluation of whether a breach creates a real risk of significant harm (s. 58(8)), and other requirements within the CPPA.

While the OPC and the courts have provided some interpretations of sensitive information, it would be preferable to have a legislative definition that sets out a general principle and is context-specific, followed by an explicitly non-exhaustive list of examples (such as those included in article 9 of the GDPR). This would provide greater certainty for organizations and consumers as to the interpretation of the term. For instance, such a definition might read:

**Sensitive information** means personal information for which an individual has a heightened expectation of privacy, or for which collection, use or disclosure creates a heightened risk of harm to the individual. This may include, but is not limited to, information revealing racial or ethnic origin, gender identity, sexual orientation, political opinions, or religious or philosophical beliefs; genetic information; biometric information for the purpose of uniquely identifying an individual; financial information; information concerning health; or information revealing an individual's geolocation.

Further, we note that the French version of PIPEDA currently refers to “renseignements … sensibles” contrary to the CPPA which proposes to rely on the term “de nature délicate”. Quebec’s Bill 64 also refers to “renseignement personnel sensible”, while the GDPR uses the term “données sensibles”. To ensure consistency with the current statute and to promote alignment with the laws of Quebec and the EU, we suggest that the French version of the CPPA revert to the term “sensible” as opposed to “de nature delicate”.

---

*Source:* Daniel Therrien, Submission of the Office of the Privacy Commissioner of Canada on Bill C-11 the Digital Charter Implementation Act, 11 May 2021.

Proposing a definition of "sensitive information" is critically aligned with digital decolonial strategy because it highlights racial sensitivity. The act of dispossession is so entwined with Colonialism that Indigenous academics like Duarte (2017) believe that the studies surrounding radicalized implications of the corporate digital infrastructure fails to acknowledge how Indigenous dispossession not only motivated settler ontologies, but still effects racialized communities today.

## Accumulation by Dispossession

The data of Indigenous communities should fall under the category of sensitive information. Mouton and Burns, in accordance with Couldry and Mejias, state that "Data colonialism combines the predatory extractive practices of historical colonialism with the abstract quantification methods of computing" because Mouton and Burns, too, believe that the social quantification of society is the act of entwining life with commodification (Couldry & Mejias, 2019, p. 337). We would be wrong to dismiss that both Colonialism and digital colonialism made colonizers wealthy. Therefore, we must analyze not only who benefits from the exploitation of data, but how and who is most disadvantaged as a result. The opposing bodies should then be treated accordingly in legislative analysis and definitions. By referencing several theorists to further explain the commodification of human life by colonizers, Couldry and Mejias

> draw to a small extent – but explicitly – on Habermas's (1989) notion of the *colonization of the lifeworld*, which they preface by stating it 'is not developed as a theory of colonialism' (2019, p. 227). Of note, authors in this field have identified several limits to this metaphorical conceptualization: most importantly,

> data are not a resource that is just awaiting discovery, but rather an asset that needs to be constructed. Along these lines, Thatcher et al. (2016, p. 994) mobilize Harvey's (2014) concept of 'accumulation by dispossession' to describe how data are produced, and then 'extracted from the producers to capture surplus value' (Mouton & Burns, 2021, p. 1892).

In summation, the authors recognize one strand of digital colonial literature that incorporates both historical and contemporary critique of capitalism, where the extraction of one actor equals the surplus value of another. If the internet is recognized as the metaphorical land of the 'New Frontier' or corporate colonizers, then data is currently being treated as a ground for that exploitation. Sensitive information, in terms of who owns it and who gets to sell it, is something that must be explored, studied, and analyzed to create a foundation of understanding that will ultimately form the basis of digital colonialism (Mouton & Burns, 2021, p. 1892).

Mouton and Burns' (2021) second strand is interrelated with the first, as it states that the current relationships humans have with digital technologies inherently reinforces strands of Colonialism, especially for racialized communities. To explain, they cite Kwet (2019) who exposed parallels between traditional colonizers and multinational technology companies who had and continue to have a hand in South African resource extraction. Mouton and Burns also cite Young because they, too, explored the concept of "fused colonialism" (a fusion of digital colonialism and Colonialism) after researching Indigenous communities in the Canadian Arctic (Mouton & Burns, 2021).

Mouton and Burns (2021) agree with Young (2019), because while they acknowledge that although transnational digital colonial research is valid, there is still a

need to "acknowledge the variety of interests *within* countries and highlight aggressive forms of data extraction that target marginalized populations inside a given country," deemed sensitive information (p. 1894). Often, theorists regard Colonialism as a global experience; however, while on some levels it is an accurate claim, it takes away from internal, smaller analyses that can expose some of the most important aspects of Colonialism. Therefore, in studying global and municipal case studies, it is no surprise that theorists of digital colonialism identify parallels (though not as physically damaging parallels) between Colonialism and digital colonialism. In both types of colonialism, sensitive information is highly valuable.

In Coleman's article whereby she refers to digital colonialism as the modern-day "Scramble for Africa," Coleman states that Kenya's 2018 Data Protection Bill is an exemplary piece of legislation because of its pursuit of decolonization. In Canada, Mouton and Burns examine their own form of colonial resistance via digital legislation by introducing Digital Neo-Colonialism, which is how "the new (neo)colonial relations necessitate re-evaluating the practices we mobilize to resist these new forms of oppression and extraction," by applying it to a Canadian consent case study: Calgary's new Smart City[15] (Mouton & Burns, 2021, p. 1894).

**Exploitation: Indigenous Digital Subjectivity and the Modernity of Colonialism**

Why is a legislative definition for sensitive information necessary? Indigenous communities do not seek the use of information communication technologies merely for

[15] Special note: In terms of smart cities and lack of consent, this is not a new or a Calgary-specific issue. Concerns around consent "has been a particularly contentious issue over the last decade. The OPCs guidance on obtaining meaningful consent has not fixed the problem. Inadequate consent was the basis for the former Ontario privacy commissioner, and Cavu Keehan, to resign from the sidewalk lab Smart city project in Toronto in mid 2018" (Phull, 2019, p. 6).

pleasure. Rather, the utility of ICTs for native communities are rooted in something substantial: resistance. This unique usage makes it sensitive. In an article on the different types of Indigenous genocide titled “Settler colonialism and the elimination of the Native” by Wolfe (2006), Wolfe states that native societies were only scarcely able to accommodate the damaging socio-economic system based on oppression that Colonial invaders introduced. The effects of colonialism continue to be felt in the previously colonized communities today, and Wolfe (2006) explains genocide and its long-term ability to eliminate radicalized citizens when he thunderously problematizes the long-lasting effects of genocide and elimination, deeming it a system “more than the summary liquidation of Indigenous people, though it includes that” (p. 390). Additionally, Indigenous data should be regarded as sensitive information because

> the logic of elimination marks a return whereby the native repression continues to structure settler-colonial society. It is both as complex social formation and as continuity through time that I term settler colonization a structure rather than an event, and it is on this basis that I shall consider its relationship to genocide (Wolfe, 2006, p. 390).

As soon as the Colonizers obtained the physical frontiers by forcibly possessing native land, the attempts to eliminate the Native did not seize there; they subsequently turned inward. The domination extended physical effects by turning psychological and digital, exploiting sensitive information that caused irreparable harm to Indigenous Communities. For settler society to function, the settlers and the subjects must deny any operation that opposes Colonial rule, lest the entire system be subject to dismantling. This

means the logic of elimination threads through the metropolitan system of today; and it is why it is so difficult to decolonize governmental structures (Wolfe, 2006, p. 393).

In the Fall of 2021, The Government of Canada vaguely addressed dismantling the system created by the settlers in Canada that ignored the importance of culturally sensitive modernization of Canada's Privacy Act. The Government stated that a modern act "could develop individualized and contextually sensitive approaches to compliance using a range of technologies" (Government of Canada, 2021, para. 16). This perspective pertains to Indigenous subjectivity and the Modernity of Colonialism explored by Wolfe (2006) and Duarte (2017), but it is not enough. In conjunction with multiple governmental departments such as the Ministry of Innovation, Science and Economic Development, the Government of Canada more specifically addressed the Indigenous concerns of Wolfe and Duarte in their article about sensitive information under the new digital revolution, titled "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians." The Government of Canada wrote:

> The Government must respect that Indigenous People are best placed to address their own challenges and must be empowered to find solutions that fit their core values and unique perspective. This is particularly true around data ownership where many Indigenous people value the principles of Ownership, Control, Access, and Possession (OCAP) and the goal of data sovereignty. Digital and data transformation has the potential to enable greater inclusion and economic participation Indigenous people that own this land. Canada must ensure that technology investments are inclusive and viewed through the lens of the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP). Canada

> must also ensure that Indigenous youth are provided the skills and training they need to succeed and that Indigenous-led businesses have access to funding and opportunities to thrive and grow (Government of Canada, mod. 2019, p. 12).

However, this report is insufficient. If it was, then Therrien's eighth recommendation to insert an official definition of sensitive information that can protect the data of Indigenous communities would not exist.

Duarte (2017) states that there are not enough studies linking contemporary tech infrastructures to settler colonial origins. In its origin, ICTs then and now were originally never meant for Indigenous use, because "In the modern settler imaginary, any Native or Indigenous use of modern technologies was unexpected precisely because Native and Indigenous peoples themselves were unexpected in the subjugated, mediated landscape" (Duarte, p. 11). Indigenous communities were not regarded as citizens; thus, they were not fairly represented in North American legislation. Therrien's recommendation 8 could distinguish the information of Indigenous communities from others could change that.

Duarte (2017) explores and explains the various ways colonialism and governmentally ordered genocide, such as the Indian Act, continues to impact Indigenous communities today. In particular, the disproportionate lack of investment in improving ICTs for Indigenous communities as opposed to other communities. The difference in treatment continues to be a contemporary issue, not a historical one (Duarte, 2017). However, Duarte emphasizes that while the disregard of ICTs in Indigenous communities is an issue, there could be a solution: and that solution could be the integration of subjective, sovereign-based legislation, such as a non-exhaustive list of demograhic-specific definitions of sensitive information. In a review of Duarte's book, Montoya

(2017) further explores Duarte's main argument about the misconceptions of ICTs and the importance of Indigenous subjectivity, stating:

> There is no totalizing discourse that can adequately address the needs of all Native communities. In fact, framing the politics of the internet as an issue of mere access allows for the settler state to paternalistically deploy itself as a benevolent savior. Instead, each community must be allowed the right to self-govern and create an ICT infrastructure that reflects the contours of its specific, geopolitical ecologies and histories. (p. 2)

The reason Indigenous subjectivity is crucial for Indigenous communities is because, unlike other communities, the need to instill sovereign boundaries over broadband network in Indigenous communities is entwined in their culture (Young, 2019). Indigenous information can potentially escape governmental regulation when deemed sensitive which should be considered a step in the right direction. Additionally, because sovereignty was intentionally stripped from them under Colonial regimes, sacred grounds belonging to Indigenous communities should not be affected by the creation of tech infrastructure. Furthermore, it is unfortunate that these communities are reluctant to demand what they want because they need to be considerate of the governments that hold the power of granting their other wishes (Duarte, 2017). We have seen governments, such as the Canadian government[16] turn on Indigenous communities for demanding

[16] In a 5-part series titled "Canada and the First Nations: A history of broken promises," author Brandy Morin explores the tumultuous relationship between the Canadian government and the First Nations. This relationship was formed and carried by the lies that were promised to the First Nations. Some of these unfulfilled promises included, but were not limited to the desist of sacred grounds, the unfair treaties, the dismissal of human rights throughout forced assimilation, and more (Morin, 2020).

sovereignty[17] time and time again. Within this context, Wolfe (2006) corrects Roger Smith's definition of genocide because Smith

> has missed this point in seeking to distinguish between victims murdered for where they are and victims murdered for who they are … So far as Indigenous people are concerned, where they are *is* who they are, and not only by their own reckoning therefore, sensitive information and Indigenous subjectivity is more than a political desire" (p. 388).

Duarte's research spotlights the fact that, unlike other Western leaders, Indigenous leaders' main concern is using telecoms to serve their people, thus only thinking of economics as a secondary purpose. It should also be noted that there are global laws set in place to acknowledge Indigenous subjectivity such as the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP), which seem to understand that the process of adding ICTs in the first place is one that must be weighed by these communities, ultimately landing on a decision that they are content with socially, politically, and economically. These sovereign categories should not be overlooked, especially since Indigenous communities experience hurdles that other communities do not face (Duarte, 2017, p. 130).

According to Duarte (2017), the dismissal of Indigenous self-governance through the buying and selling of their sensitive data is a reinforcement of Colonial tactics to control inward and outward aspects of life. This type of decolonial topography study addresses Indigenous subjectivity and "reorients the technique of applied science toward

[17] Currently, in the United States of America, several tribes have deemed the universal access to network so unsatisfactory, that they are taking network distribution into their own hands and creating their own service providers. One of these initiatives is called Tribal Digital Village network (Curl, 2022).

meeting the goals of tribal communities," an admirable goal for a country that claims they are dedicated to reconciliation (Duarte, p. 136). The operative term, should the Canadian government want to use it, is self-sufficiency, and the legislative failure of Indigenous peoples in North America is an important example of why current legislation must consider the effects of Colonialism, such as where extraction, dispossession, and exploitation are concerned). One of Young's (2019) central arguments was the importance of Indigenous subjectivity in data legislation. Because settler Colonialism had the goal of Indigenous elimination and commodification, its effects were detrimental and meant to be long-term. Nevertheless, Indigenous people are expected to fall under the category of "consumers" in Canadian legislation like Bill C-11. However, Indigenous communities are not like other communities. The inherent biases imbedded in algorithms pave the way for all data produced by Indigenous communities to be potentially harmful and, if Therrien's definition was an accepted amendment, categorized as legally "sensitive."

Amending the CPPA to refine the definition of sensitive information using clear language and various context-based examples could help build trust for external governments and Indigenous communities. Aside from the fact that Recommendation #7 deemed inferred information sensitive information, there are many reasons why a legislative definition of sensitive information is both necessary and non-negotiable, especially where biometric data previously used for predictive policing (explained more on page 33) and Indigenous genocide is concerned.

The repercussions of Indigenous genocide is still felt by Indigenous communities today, rendering their communities vulnerable (Wolfe, 2006). Wolfe (2006) stresses the

fact that Indigenous genocide was both mentally and physically detrimental, as it was not an event but a long-term structure of governance that was made to exceed physical boundaries. Indigenous communities should not have to consent to anything from external organizations. But if they must, then requiring a sensitive information clause that a reasonable *Indigenous* person under subsection 12(2)(a) must confirm is a start. Most notable of all from Recommendation #8 is the use of the term "context-specific" subsections in amended definitions, because if there is subjective, autonomous context tailored completely to Indigenous peoples, who are recognized as having an independent knowledge system, then they would be given the tailored tools to make an informed decision as to whether they agree to data extraction or not. This is a substantial difference when compared to the last time an external governmental group extracted their lands and exploited their labour without their consent. Again, this is not enough, but it is a start. It is important to note that unlike how the catchall term "organization" in Bill C-11 accounts for advertising agencies and governments alike, Bill C-11's categories "organization" "consumer," "reasonable person[18]," and "general principle" are not one-size-fits-all terms. Due to having different knowledge systems, Indigenous communities, in many ways, do not abide by the same politics as the rest of the communities in their category (Young, 2019).

A context-specific definition of sensitive information alongside numerous examples would better equip extractees for subjective, emotional analysis upon Indigenous-approved specific terms and conditions. Colonizers benefit from digital

[18] In Tort Law, "the reasonable person is a hypothetical person used as a legal standard to determine whether the conduct of the parties in a case was proper in the circumstances. It is the standard of conduct adopted by persons of ordinary intelligence and prudence" (Courthouse Library British Columbia, 2019).

colonialism by commodifying the sociality of consumers and accumulating it through dispossession. Therefore, to deny Indigenous communities the best tools for analyzing of their dispossession is to undermine their right to combat an unfair economic process through decoloniality (Mouton & Burns, 2021). Data collection, at some level, can be compared to the Scramble for Africa in terms of its lack of consent from extractees (legally known as consumers) (Coleman, 2019). Something that is clear to a "reasonable person" could differ greatly from that of a "reasonable Indigenous person" because of the distinctive way each Indigenous community operates. Unlike other racial minorities, consenting to sharing sensitive information for Indigenous communities is likely for the purpose of utilizing ICTs for resistance and culture perseverance, not just for enjoyment (Young, 2019). There is a critical emotional unit of analysis needed from Indigenous communities prior to giving their valid consent, which should be addressed as a context-specific section of the amended definition of "personal information."

***Recommendation 11:*** *That subsection 15(3) of the CPPA be amended as follows: The individual's consent is valid only if, at or before the time that the organization seeks the individual's consent, it provides the individual with the following information, in a manner such that it is reasonable to expect that the individual would understand the nature, purpose and consequences of the intended collection, use or disclosure. This information must be presented in an intelligible and easily accessible format, using clear and plain language.*

---

*Source:* Daniel Therrien, Submission of the Office of the Privacy Commissioner of Canada on Bill C-11 the Digital Charter Implementation Act, 11 May 2021.

***Original Subsection 15(3):***

***Information for consent to be valid***

***(3)*** *The individual's consent is valid only if, at or before the time that the organization seeks the individual's consent, it provides the individual with the following information in plain language:*

***(a)*** *the purposes for the collection, use or disclosure of the personal information determined by the organization and recorded under subsection 12(3) or (4);*

***(b)*** *the way in which the personal information is to be collected, used or disclosed;*

***(c)*** *any reasonably foreseeable consequences of the collection, use or disclosure of the personal information;*

***(d)*** *the specific type of personal information that is to be collected, used or disclosed; and*

***(e)*** *the names of any third parties or types of third parties to which the organization may disclose the personal information.*

---

*Source:* Daniel Therrien, Submission of the Office of the Privacy Commissioner of Canada on Bill C-11 the Digital Charter Implementation Act, 11 May 2021.

Although closely related to Recommendation 8, Recommendation 11 is critical for Indigenous subjectivity because indisputable consent should be required by extractees to be considered ethical. If the terms and conditions of consent are written in plain,

unambiguous language understandable by all, then one may assume that Indigenous communities and all communities may be able to properly decide if granting permission for data extraction is in their best interest or not. This would be a respectable decolonial gesture in the digital sense, that was, unsurprisingly, not offered in Colonial regimes. As was explained by Gitelman on page 18, if the pros and cons of data extraction information is not specific, explicit, and legitimate to all actors, then it runs the risk of being an act of domination through the use of ambiguous terminology. Every word in legislation is critical to the way data will be treated, and Griziotti (2018) calls this exploitation a form of unfortunate digital deterritorialization[19].

## The Scramble for Africa[n Data]

While Couldry and Mejias (2019), at large, utilize Indigenous case studies to explain digital colonialism, Coleman (2019) more specifically explores the African example regarding the long-term effects in their article "Digital Colonialism: The 21st Century Scramble for Africa Through the Extraction and Control of User Data and The Limitations of Data Protection Laws." Coleman's article dedicates an entire section to defining digital colonialism, relating it to the Colonization of the African continent by exposing who the modern colonizers are under digital colonialism:

> Earlier colonialists arrived on African shores to expand their empires by exploiting local labor to extract valuable natural resources and raw materials, building critical infrastructure like railroads in the process to facilitate the import and export of these often dispossessed goods. Today's colonialists, however, are digital. They build communication

[19] Deterritorialization is "the severance of social, political, or cultural practices from their natuve places and populations" (Oxford Languages, n.d).

> infrastructures such as social media platforms and network connectivity for the express purpose of harvesting data, churning a profit, and/or storing the data as raw material for predictive analytics (p. 422).

In other words, Coleman (2019) deems modern digital colonizers actors one and three, the tech corporations and governments. They are the bodies that build the contracts. What is interesting about comparing digital colonialism, Colonialism, and Bill C-11, is the explicit commonality around the murkiness of consent. Data extraction –similar to African soil—is the decentralized theft of valuables that were taken with or without the explicit consent of the individuals who own it (Coleman, 2019, p. 422). For instance, resource extraction in Africa may have served the purpose of building Western infrastructure; however, it was unwelcome and unwanted infrastructure to the benefit of the colonizers. An example of this would be the investment in transportation infrastructure in Africa that resulted in the prevalence of trains; however,

> Such investments were strictly for the benefit of facilitating the efficient transport of raw materials and not for the enrichment of the countries themselves. Simply put, the infrastructure that was developed was designed to exploit the natural resources of the colonies (Coleman, 2019, p. 420)

As Colonial history has proven, there was an unwelcome and one-sided agenda in Colonial endeavours. This agenda was often to the benefit of colonizers for their economic gain, similar to the manner in which the agenda of digital colonialism economically benefits the digital colonizers, corporations (1), advertising companies (2) and governments (3). Additionally, consent should be well-informed, active, conditional, and capable of being revoked at any point in time. In other words, valid consent should

be as valid as it can be, but how? According to Recommendation #11 by OPC, valid consent can only be considered valid if it responds "*in a manner such that it is reasonable to expect that the individual would understand the nature, purpose and consequences of the intended collection, use or disclosure. This information must be presented in an intelligible and easily accessible format, using clear and ~~in~~ plain language."* An amendment that explain the pros, cons, and validity of consent could mitigate the detrimental effects of digital colonialism.

**Recommendation 15:** That s. 39 of the CPPA be amended to require:

- A written request be made prior to information being disclosed to ensure that the use is of societal benefit as defined in the CPPA;
- An information sharing agreement be entered into, which would prohibit the recipient from re-identifying the information as well as from using the information for secondary purposes which are not of a societal benefit; and
- The definition of "socially beneficial purposes" should be amended to include a limit on regulatory power, for example by indicating that they must be "purposes that are beneficial to society and not simply of individual or commercial interest or profit."

---

*Source:* Daniel Therrien, Submission of the Office of the Privacy Commissioner of Canada on Bill C-11 the Digital Charter Implementation Act, 11 May 2021.

***UNEDITED subsection 39:***

***Socially beneficial purposes***

***39 (1)*** *An organization may disclose an individual's personal information without their knowledge or consent if*

***(a)*** *the personal information is de-identified before the disclosure is made;*

***(b)*** *the disclosure is made to*

***(i)*** *a government institution or part of a government institution in Canada,*

***(ii)*** *a health care institution, post-secondary educational institution or public library in Canada,*

***(iii)*** *any organization that is mandated, under a federal or provincial law or by contract with a government institution or part of a government institution in Canada, to carry out a socially beneficial purpose, or*

***(iv)*** *any other prescribed entity; and*

***(c)*** *the disclosure is made for a socially beneficial purpose.*

***Definition of socially beneficial purpose***

***(2)*** *For the purpose of this section,* ***socially beneficial purpose*** *means a purpose related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose.*

---

*Source:* Daniel Therrien, Submission of the Office of the Privacy Commissioner of Canada on Bill C-11 the Digital Charter Implementation Act, 11 May 2021.

The term 'socially beneficial purposes[20]' has a positive connotation in that it calls for a fair and ethical relationship between consumers and their data. The 'socially beneficial purpose' of data collection would make data collection beneficial for all 4 actors instead of just 1, 2, and 3. A socially beneficial purpose will stimulate competition, reduce discrimination, and level the digital playing field (Pinto, 2021).

**Nation-to-Nation Digital Domination: China and The West vs. No One**

In their work, "Digital Sovereignty or Digital Colonialism?" Pinto (2021) argues that both digital sovereignty (one's ability to do as they please and own what they create in digital spaces) and digital colonialism can and should be redressed through the development of proper legislation. By Pinto's definition, digital colonialism is the idea that "almost every activity is mediated by our interaction with technologies and services offered by an increasingly concentrated conglomerate" (p. 19). Therefore, it undermines digital sovereignty because if a conglomerate has more control over our data than ourselves, there is a problem for everyone; but especially communities who have fought for sovereignty on and off the internet (Pinto, 2021, p.19).

Pinto's (2021) foregrounding of the political economy of digital colonialism is similar to Coleman's (2019) because they situate Western countries as integral actors facilitating digital colonialism by "investing heavily in research and development, not only to maintain their dominant position in the industry and to aggressively expand to as

[20] In general, something that is socially beneficial means "the increase in social welfare that results from taking an action. Social benefits include private benefits and those benefits not taken into consideration by private decision makers in the actions they choose to take, including effects occurring in the future. Benefits valuation involves measuring the physical and biological effects on the environment from the actions taken. Benefits are generally treated one or more of three ways: A narrative containing a qualitative discussion of environmental effects, a quantified analysis expressed in physical or biological units, and a monetized benefits analysis in which dollar values are applied to quantified physical or biological units" (Law Insider, n.d.).

many markets as possible, but also to explore innovative ways to integrate information technology in every aspect of the public administration, the private sector, their defence and security, and the application of citizen rights" (Pinto, 2021, p. 17). The tech empires' current market expansion is a perfect example of their pursuit of profit by the dispossession of citizens' data, otherwise known as secondary purposes, that are not to the benefit of society but the benefit of their commercial profit. Due to this expansion of ownership, a central argument in the article "Digital Sovereignty or Digital Colonialism?" is the creation of a global system of technological dependency. In this argument, underserved countries, those lacking digital infrastructure compared to the West, and overserved countries, in terms of having the most ownership over digital infrastructure, are at odds, with the underserved countries being dependent on the data regulations of the overserved because the overserved simply own all the major platforms the citizens are on. The big tech companies, sometimes referred to as tech empires like Facebook and Google, have the means and the lawyers to create world-dominating platforms that eliminate competition, despite competition being democratic in nature. Tech empires' capital unlocks access to resources, architecture for business, and intellectual resources that make it virtually impossible to catch up to the leaders (Pinto, 2021). Technological dependency might be long-lasting, because some regions have instilled restrictive legislation that does not support a competitive digital market. For instance,

> Such restrictions only increase, with little possibility of reversal, due to the new group of Free Trade Agreements the Trans Pacific Partnership (TPP), Transatlantic Trade and Investment Partnership (TTIP), and Trade in Services

> Agreement (TISA), [but] some of the provisions of the new generation trade agreements even consider tighter privacy laws and policies in a country as a barrier for trade, disregarding the superiority of human rights laws over any other law (Pinto, 2021, p.17).

The fact of the matter is that platforms from underserved countries do not have the disposable finances or tools to keep up with the giants in the West. When the West was expanding their technological reach through the telegraph in the late 19th and the early 20th centuries, underserved communities were busy fighting against their genocide. These communities were unlikely to win a race they were not allowed to participate in. These communities were not allowed to participate because "the general rule was that for Americans to prosper, Indians had to die" (Duarte, 2017, p. 11). Thus, the underserved have no choice but to succumb to the terms and conditions of the tech empires. A gap that is of disadvantage to so many exemplifies the dangers of companies which are not generally beneficial to society. In the Global South, external tech companies enjoy full control over social data accumulated on their platforms, leaving already underserved countries in a vulnerable position. A lack of technological education and technological funding induces a radical system of technological dependency, comparative to the dependency theory[21] caused by Colonialism. The pre-established system of dependency makes underserved countries vulnerable and relatively unchallenging areas to dominate by the West and China (Pinto, 2021). Western and Chinese tech empires "are currently engaged in aggressive pushes to invest in areas which traditionally belonged to the state

[21] Dependency Theory is "the unequal exchange relationship between developed and developing countries viewed as contributing to poor economic growth. Dependency theory focused on individual nations, their role as suppliers of raw materials, cheap labor, and markets for expensive manufactured goods from industrialized countries" (Science Direct, 2022, para. 2).

or other specialized agencies and providers," which will create an unhealthy monopoly only managed by the tech empires (Pinto, 2021, p. 17). Even more concerning is that tech monopolies are a constant source of political pressure on underserved countries, strong arming them into decisions and threatening to pull resources and aid if they are not compliant. Therefore, the remnant of Colonial feudalism ensures that any pushback can never be an act of total independence (Pinto, 2021, p. 17). Pinto believes that countries and communities most affected by Colonialism present a susceptible terrain for data-conglomerate domination. From her article "Dark Google" Pinto cites expert professor Shoshana Zuboff who, concerning digital colonialism, "warns of the dangers of revolving doors between the largest companies and their governments, which might be tempted to use technology to their geopolitical advantage" (in Pinto, 2021, p. 18).

Griziotti explains that dispossession derived from a toxic social contract put forth by governments who did not have their citizens' best interests at heart. Similar to Colonizers, the dispossession of land was not perpetuated in the interests of the people whose lands they belonged to. Because of this, the 15th recommendation that "The definition of "socially beneficial purposes" should be amended to include a limit on regulatory power, for example, by indicating "purposes that are beneficial to society and not simply of individual or commercial interest or profit" could tangibly, this entail instating a community-based system of checks and balances (Therrien, 2021). Furthermore, separating "socially beneficial purposes" from "socially beneficial purposes for racialized people" could improve this recommendation because:

> There's been a growing swell of concern in the academic community about the stranglehold that commercial (for-profit) search engines have over access to

> information in our world. Noble builds on this body of work...to demonstrate that search engines, and in particular Google, are not simply imperfect machines, but systems designed by humans in ways that replicate the power structures of the western countries where they are built, complete with all the sexism and racism that are built into those structures. (50 Best Books of 2018 in Noble, 2018, para. 10)

Algorithms are intrinsically discriminatory and prejudicial, so they are not societally beneficial. And if we take something that is more widely regarded as a societal issue such as climate change, data extraction still presents a serious problem. Griziotti (2018) explains that

> Much irrecoverable damage can stem from the effects of data extraction, as told by indignant critics [who] predict dire consequences for the future of the biosphere and humanity … these consequences are due to the profound deterioration caused by decades of capitalist practice incarnated in the neoliberal organization of cognitive labor. (p. 46)

Neoliberal practices like data extraction are inherently individualistic, so for Therrien to call for a Bill C-11 amendment limiting regulatory power is extremely significant. Recommendation 15 not only acknowledges the imbalance of power between organizations and consumers, but it attempts to mitigate that imbalance caused by digital colonialism by requiring those in power to act in the best interest of the societal collective. Requiring those in power (the organizations) to act in the best interest of the society as opposed to acting only in the interests of individual and commercial interests

of their organizations is one step toward dismantling the social quantification sector and is, by extension, a proper decolonial gesture.

### My Bill C-11 Recommendation: The Prosumer Privacy Protection Act

In his article "Prosumer Capitalism," Ritzer (2015) explains the longstanding existence of prosumption (and prosumers[22]) despite many believing it is a new concept. He states that

> Production and consumption have always been prosumption processes or, to put it the other way, prosumption is a hybrid act involving a mix of production and consumption. There is no such thing as either pure production (without at least some consumption) or pure consumption (without at least some production); the two processes always interpenetrate. This is the case when whichever one—production or consumption—seems to pre-dominate in any particular setting and at any given point in history. Even if they did not have the concept, sociologists, social theorists, and other students of society should have always focused on prosumption. At best, production and consumption should have been treated as special limiting cases of prosumption, as "ideal types." (p. 414)

I suggest including prosumption in the amended Bill because this MRP is an analysis of a 'Consumer' Privacy Protection Act when I personally believe it should be regarded as the 'Prosumer' Privacy Protection Act. One major detrimental long-term effect of Colonial jurisdiction was the colonizer's inability to see colonized peoples as both producers and consumers, fueling the groundwork for Colonial slave labour and digital colonial unpaid labour. Under Colonialism and digital colonialism, there are

[22] A prosumer, in this context, is an actor who consumes and also produces. According to Arimetrics, the glossary for all things digital, "a **prosumer** is a fusion of the words product and consumer. The term was coined by **writer Alvin Toffler**, who mentioned it in his book 'The Third Wave', from 1980. Although historically it has been used in very different areas, in the world of technology and digital marketing refers to the user who is both a consumer and a creator of content on websites and social networks" (2022, para. 1).

bodies who produce (the colonized / actor 4) and people who benefit from that production (Colonizers / actors 1, 2, & 3). This mislabeling is present under the theory of extraction, exploitation, and dispossession. While many theorists, communication researchers, political analysts and academics alike have rightfully exposed the various issues with the term 'consumer' during the Bill C-11 panel Towards a New Privacy Deal? Hot Takes from Privacy Experts on C-11 (2020), none had explicitly highlighted the overlook of prosumer relations in Colonialism, digital colonialism, and Canadian digital legislation. Similarly, and in addition to his takes on that panel, Michael Geist stated that one of the errors of other Canadian digital legislations was the fact that it failed to regard the individual users (consumers) as broadcaster (producers) (Geist, 2022, para.3). In my opinion, it is time that seeing consumers as both producers and consumers is applied to legislation, especially highly critiqued legislation that has received much backlash like Bill C-11, lest the legislation is engaging in a dismissal of labour. To see consumers as prosumers is a decolonial gesture.

A citizen that is both a data consumer and a producer is a prosumer (Griziotti, 2018, p. 39). However, there are many reasons why refusing to acknowledge that Canadians that produce data are labourers by only seeing labourers as data plains is doing a disservice to their work. Couldry and Mejias (2019) believe that social interactions online should be treated as valuable work because of its profitability. It is the reason tech companies are so successful. The fact that consumers are not referred to as both consumers and producers is, I believe, a central reason that Bill C-11 has garnered so much criticism. Griziotti argues that the strongest chance at resistance that humanity has to avoid a labour collapse, in which mistreated and mislabeled labourers are forced to

combat their managers in a soft proletariat revolution at the cause of too much exploitation would be to appoint consultants and experts who can stop policies that are at large unhelpful to the multi-dimensional labourer (2018). In this light, I strongly believe theorists such as Griziotti, Couldry and Mejias would support experts such as Daniel Therrien pushing a recommendation that calls for the changing the labelling of 'consumers' to 'prosumers' in the current Consumer Privacy Protection Act.

**Amending Amendments: Final Word**

Since this paper can only provide a limited amount of insight into the issues of Bill C-11, I think one of the reasons Bill C-11 falls short of digital colonialism sensitivity is because Bill C-11 is not tackling the right issues. While it adequately addresses Canadian content, it fails to adequately address the Colonial aspects of the Canadian digital infrastructure. Luckily, Therrien's four recommendations above, do. However, what is needed now is an actual digital colonial analysis. While I agree with much of what is provided in Therrien's suggestions, I think it could be enhanced by examining through this conceptual lens. Unlike Therrien's recommendations, I would like to see recommendations that address digital colonialism head-on. These must be digitally decolonial.

As detailed in legal researcher Phull's (2019) book *Big Data Law in Canada,* despite being written prior to the Bill C-11 proposal, Phull stated that all data legislation should abide by the following ten regulatory principles: Accountability; Identifying Purpose for Collection; Consent; Limiting Collection; Limiting Use, Disclosure, and Retention; Accuracy; Safeguard; Openness; Individual Access, and Challenging Compliance (p.5).

The above ten privacy principles may appear conceptually simplistic; however, in the history of their application in Canadian data law, they were deceptively complicated for the purposes of ignorant compliance (Phull, 2019, p. 6). Phull states that consent (or the lack thereof), is a major link between Colonialism and digital colonialism and was supposed to be clarified and strengthened in current legislation - which could very well have included legislation such as Bill C-11. However, that is not the case in Bill C-11, hence why Therrien's recommendations call for clarification, outright revision, a completely reworded preamble, and an improved articulation aligned with the regulatory principles.

## Why The Concern?

Sovereignty is the opposite of colonization. Digital sovereignty, the ability to oversee one's own data, is crucial because the effects of digital colonialism are attached to an extensive, toxic infrastructure more prominent than itself (Duarte, 2017). Canada and other countries will have difficulty detaching themselves from digital colonialism's toxicity because the current constitutions, laws, and policies are not being amended often enough, if at all, to make a difference (Pinto, 2021). Pinto (2021) argues that digital decolonial policy analysis is required in a world in which it should be more important than ever. She states,

> Public policies should be enacted to guarantee that the adoption of new technologies at a massive scale does not create further inequality, exclusion, or imposition of values and practices that are foreign to the host communities. Instead, it could be an opportunity to rescue and develop further local knowledge.

> Rooted in the local, in the decentralized and in the digital commons logic: these characteristics of the current policies will defeat digital colonialism (p. 23)

A solution to these issues is digital sovereignty. Constitutions should guarantee Indigenous autonomy over digital infrastructure because digital sovereignty would leave the inhabitants of a particular geographical area in charge of where their data goes, or if it leaves their possession at all. If states want to fix the issues connected to digital colonialism, states would be wise to appoint actors who can educate the citizens, strengthen human resources and invest in local digital colonial research initiatives, before ignoring self-governance (Pinto, 2021). In doing so, "this will gradually enable a culture of digital dignity with human rights standards embedded in protocols at the regional and international level" (Pinto, 2021, p. 23). I take the position that Bill C-11 suffered (and continues to suffer) backlash because it failed to adequately address multiple issues regarding user-generated content. However, I believe the issues that go the most unnoticed are the ones in regards to digital colonialism. An amended Bill C-11 should acknowledge the role of digital colonialism and be given significant amendments "to start addressing global digital inequalities and embrace a future that places digital autonomy and human dignity at its core, social innovation should be encouraged and institutionalised at the community and citizen level to guarantee its scalability and permanence" (Pinto, 2021, p. 23). Therrien has stated the same.

As previously discussed, Indigenous subjectivity must be embedded and put forth by contemporary legislation, such as Recommendations 7, 8, 11 and 15. I postulate that by creating a body independent of the OPC that has a sole task on focusing on restructuring and educating Canadians on digital colonialism; then my inquiries can be

explicitly posed and perhaps improvements can be made to the Consumer Privacy Protection Act.

## Conclusion

In this paper, I have applied the theoretical framework of digital colonialism to four of the OPC's proposed amendments of the recent Consumer Privacy Protection Act: Bill C-11. Through a literature review of the definition, I answered my first research question, *What is digital colonialism?* By finding the definition that best encapsulates the theoretical framework. Then, by using Couldry and Mejias' (2019) definition, I explored my second research question: *How, from a digital colonial standpoint, can we unpack recommended amendments 7, 8, 11* and *15 proposed by the previous Office of the Privacy Commissioner?* A proportional, interpretive policy review of the OPC's four promising recommendations that I deemed indirectly touching on digital colonialism, (7 on inferred information, 8 on sensitive information, 11 on accessible information for permissible consent and 15 on socially beneficial purposes) was conducted.

Through the exploration of both the Bill and the theoretical framework of digital colonialism, I was able to contend that Bill C-11 was (and continues to be) ill-received because it does not aim to dismantle digital colonialism. In my view, Bill C-11 did not go over well because of its failure to address toxic, lasting elements of Colonialism. On the digital frontier, it is no coincidence that African and Indigenous academics alike have called for political digital colonial examination. And as a descendent of colonized nations myself, this paper is an execution of my attempt to do just that as it is my do-ocractic duty as a digital-decoloniality researcher.

It is unrealistic to consider the abolition of digital colonizers the same way colonizers were abolished because the value of data is different compared to the value of oil. However, even with the invention of smart cars and smart cities, resources will still require years to phase out. That being said, many of the communication experts mentioned in this paper, including the computer scientist Griziotti (2018), call for legislative reform that addresses digital colonialism. Griziotti argues that without legislative reform, a country is playing with the health of their welfare state both figuratively and literally; both intangibly and intangibly; both cognitively and biologically; much like a viral (or digitally viral) contagion that consumes collateral victims. Perhaps one could say the persistence, longevity, and illness-like spread of Colonialism are comparable to a digital pandemic; however, though as apprehensive about the future of digital legislation in Canada as I may be, I will wait for the subsequent amendment following Therrien's recommendations of Bill C-11 before I, myself, call it that.

## REFERENCES


Aiello, R. (2023). What is going on with Bill C-11, the government's online streaming legislation? *CTV News.* https://www.ctvnews.ca/politics/what-is-going-on-with-bill-c-11-the-government-s-online-streaming-legislation-1.6249113

Algorithms of oppression: How search engines reinforce racism. (2021). *Science.* Vol 374, Issue 6567. DOI: 10.1126/science.abm5861

What is a prosumer. (2022). *Arimetrics.* https://www.arimetrics.com/en/digital-glossary/prosumer

Bains, N. (2021). Bill C-11 (historical). *Open Parliament.* https://openparliament.ca/bills/43-2/C-11/

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code.* Polity.

Bill C-11: *An act to enact the consumer privacy protection act and the personal information and data protection tribunal act and to make consequential and related amendments to other Acts.* (2020). 1st reading Nov. 17, 2020, 43rd Parliament, 2nd session.

Canada's System of Justice. (mod. 2021). Modernizing Canada's privacy act. *Government of Canada.* Retrieved from the Government of Canada website: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html?wbdisable=true

Canadian Charter of Rights and Freedoms. (1982). Part 1 of the Constitution Act, being Schedule B to the Canada Act 1982 (UK), c 11.

Canadian Press. (2020). Use of predictive policing tools in Canada highlight need for federal action, report says. *CityNews Everywhere.*

https://ottawa.citynews.ca/amp/national-news/use-of-predictive-policing-tools-in-canada-highlight-need-for-federal-action-report-says-2679133

CBC. (2020). “We were told we kept our freedom.” Canadians have been breaking their promises to Indigenous people. *CBC DOCS POV.* https://www.cbc.ca/cbcdocspov/features/we-were-told-we-kept-our-freedom-canadians-have-been-breaking-their-promis

CDTS / CLTS uOttawa. (2020). *Towards a new privacy deal? Hot takes from privacy experts on C-11* [Video]. YouTube. https://www.youtube.com/watch?v=43cbf4tgp94&t=3665s

Coleman, D. (2019). Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race & Law*, 24(2), 417–439.

Connell, R. (2010). *Southern theory: The global dynamics of knowledge in social science.* Polity.

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism.* Stanford University Press.

Chartered Professional Accountants Canada. (n.d). Daniel Therrien. *Chartered Professional Accountants Canada.* https://www.cpacanada.ca/en/career-and-professional-development/event-biographies/daniel-therrien

Curl, M. (2022). Native americans long ‘left out’ from broadband push for equity. *Bloomberg Government.* https://about.bgov.com/news/native-americans-long-left-out-from-broadband-push-for-equity/

Davis, K. (2013). The rise of social media as a career. *Entrepreneur.* https://www.entrepreneur.com/science-technology/the-rise-of-social-media-as-a-career-infographic/228651

Digital First Canada. (2022). *About digital first canada.* https://digitalfirstcanada.ca/about/

Duarte. (2017). *Network Sovereignty: building the Internet across Indian Country* (1st edition.). University of Washington.

Dyer-Witheford, N. (1999). *Cyber-Marx.* Urbana: University of Illinois Press.

Geist, M. (2022). Not ready for prime time: Why bill C-11 leaves the door open to CRTC regulation of user generated content. *Michael Geist.* https://www.michaelgeist.ca/2022/02/not-ready-for-prime-time/

Gitelman, L. (2013). *Raw data is an oxymoron.* The MIT Press.

Electronic colonialism. (2021). In *Wikipedia*. https://en.wikipedia.org/wiki/Electronic_colonialism

Griziotti, G. (2018). *Neurocapitalism: Technological mediation and vanishing lines.* Minor Compositions.

Habermas. J. (1989). *The theory of communicative action.* Vol. 2. 196. Cambridge, UK: Polity.

Harvey, D. (1996). *Justice, nature and the geography of difference.* Oxford, UK: Blackwell Publishers.

Innovation, Science and Economic Development Canada. (2018). Canada's digital charter in action: A plan by Canadians, for Canadians. Retrieved from the

Government of Canada website: https://ised-isde.canada.ca/site/innovation-better-canada/sites/default/files/attachments/Digitalcharter_Report_EN.pdf

Innovation, Science and Economic Development Canada. (mod. 2019). Canada's digital charter in action: A plan by canadians, for canadians. Strengthening privacy for the digital age: proposals to modernize the personal information protection and electronic documents act. Retrieved from the Government of Canada website: https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/strengthening-privacy-digital-age

Jacksch, E. [SecurityGuy]. (2021, March 31). *Bill C-11 (Canada, 2021)* [Video]. Youtube. https://www.youtube.com/watch?v=MF5eqUKNqAo&t=7s

Kavya. (2021). Canada's new privacy law: the consumer privacy protection act (CPPA). *Cookie Law Information.* https://www.cookielawinfo.com/canadas-consumer-privacy-act-cppa/

Kohn, M., & Kavita, R. (2023). "Colonialism." *The Stanford Encyclopedia of Philosophy* (Spring 2023 Edition), Edward N. Zalta & Uri Nodelman (eds.). https://plato.stanford.edu/archives/spr2023/entries/colonialism/

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the global south. *Race & Class*, 60(4), 3–26. https://doi.org/10.1177/0306396818823172

Law Insider. (n.d.). Social benefits definition. In *LawInsider.com.* https://www.lawinsider.com/dictionary/social-benefits

Mann, M., & Daly, A. (2019). (Big) data and the north-in-south: Australia's informational imperialism and digital colonialism. *Television & New Media*, 20(4), 379–395. https://doi.org/10.1177/1527476418806091

Montoya, S. A. (2019). Review of network sovereignty: building the internet across Indian country, Marisa Elena Duarte. *Catalyst* (San Diego, Calif.), 5(2). https://doi.org/10.28968/cftt.v5i2.31966

Morin, B. (2020). Canada and the First Nations: A history of broken promises. *Aljazeera.* https://www.aljazeera.com/features/2020/3/17/canada-and-the-first-nations-a-history-of-broken-promises

Mouton, M., & Burns, R. (2021). (Digital) neo-colonialism in the smart city. *Regional Studies*, 1–12. https://doi.org/10.1080/00343404.2021.1915974

Mulderrig, J., Montesano Montessori, N., & Farrelly, M. (2019). *Introducing critical policy discourse analysis.* Cheltenham, UK: Edward El- gar Publishing. https://doi.org/10.4337/9781788974967.00006

Mumford, L. (1934). *Technics and Civilization.* New York: Harcourt, Brace and Company.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism.* New York University Press.

New World Encyclopedia. (2023). Scramble for Africa. In *New World Encyclopedia.* https://www.newworldencyclopedia.org/p/index.php?title=Scramble_for_Africa&oldid=1097851

Office of the Privacy Commissioner of Canada. (2013). Individual objects to the real-time accuracy of credit score. PIPEDA Report of Findings #2013-008. Retrieved from the Office of the Privacy Commissioner of Canada website: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-008/

Office of the Privacy Commissioner of Canada. (mod. 2015). Accidental disclosure by Health Canada. Retrieved from the Office of the Privacy Commissioner of Canada website: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2014-15/pa_20150303/

Office of the Privacy Commissioner of Canada. (2021). Guidelines for obtaining meaningful consent. Retrieved from the Office of the Privacy Commissioner of Canada website: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

Oxford Languages. (n.d). Deterritorialization. *In Oxford Languages.*

Parsons, C. (2021). Canada's proposed privacy law reforms are not enough: A path to improving organizational transparency and accountability. *The Citizen Lab: University of Toronto.* https://citizenlab.ca/2021/04/canadas-proposed-privacy-law-reforms-are-not-enough-improving-organizational-transparency-and-accountability-bill-c11/

Phull, C. (2019). *Big data law in Canada.* Smartblock Law Professional Corporation.

Pinto, R. (2021). Digital sovereignty or digital colonialism? *International Journal on Human Rights,* 15(27), 15–.

Ritzer, G. (2015). The "new" world of prosumption: evolution, "return of the same," or revolution? *Sociological Forum* (Randolph, N.J.), 30(1), 1–17. https://doi.org/10.1111/socf.12142

Srnicek, N. (2017). *Platform capitalism.* Polity Press.

Stingl, A. I. (2016). *The digital coloniality of power: Epistemic disobedience in the social sciences and the legitimacy of the digital age.* Lexington Books.

Taffel, S. (2021). Data and oil: Metaphor, materiality and metabolic rifts. *New Media & Society*, 146144482110178–. https://doi.org/10.1177/14614448211017887

Thatcher, J., O'Sullivan, D., & Mahmoudi, D. (2015). Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning. D, Society & Space*, 34(6), 990–1006. https://doi.org/10.1177/0263775816633195

Therrien, D. (2021). Submission of the office of the privacy commissioner of canada on bill C-11, the digital charter implementation act, 2020. Retrieved from the Office of the Privacy Commissioner of Canada website: https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/

User Centrics. (2021). Canada's consumer privacy protection act – an overview. *Usercentrics.* https://usercentrics.com/knowledge-hub/canada-consumer-privacy-protection-act/

Warburton, M. (2021). New privacy bill won't fix Canada's longstanding issues, critics say. *Global News*. https://globalnews.ca/news/7879632/privacy-bill-c11-problems/

Winseck, D. (2022). Still not dead: why legislators should kill the online streaming act. *Centre for International Governance Innovation.* https://www.cigionline.org/articles/still-not-dead-why-legislators-should-kill-the-online-streaming-act/

Wolfe, P. (2006). Settler colonialism and the elimination of the native. *Journal of Genocide Research,* 8(4), 387-409, DOI: 10.1080/14623520601056240

Young, J. C. (2019). The new knowledge politics of digital colonialism. *Environment and Planning.* A, 51(7), 1424–1441. https://doi.org/10.1177/0308518X19858998

Zimmer, B. (2018). Towards privacy by design: review of the personal information protection and electronic documents act. 42nd parliament, first session. Retrieved from the House of Commons website: https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf

## VITA AUCTORIS

| | |
|---|---|
| NAME: | Kayla Clarke |
| PLACE OF BIRTH: | Ottawa, ON |
| YEAR OF BIRTH: | 1997 |
| EDUCATION: | Stanstead College, Stanstead, QB, 2015 |
| | University of Windsor, B.A., Windsor, ON, 2020 |
| | University of Windsor, M.A., Windsor, ON, 2023 |