BLINDED BY TRANSPARENCY:

AI Disclosure Practices in the Canadian Financial Industry

MAURA HANLEY

THESIS SUBMITTED IN PARTIAL FULLFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF ARTS

YORK & TORONTO METROPOLITAN JOINT GRADUATE PROGRAM IN COMMUNICATION & CULTURE
YORK UNIVERSITY,
TORONTO ONTARIO

MAY 18, 2023

ABSTRACT

This thesis investigates transparency practices related to the governance and communication of the use of artificial intelligence (AI) in the Canadian banking industry through a case study of Canada's five largest banks. By asking how AI and data practices are framed and communicated, what beliefs and values are expressed, and what are the implications for public trust and future policy, this thesis challenges our reliance on transparency as a form of governance. The study employs a multi modal approach, evaluating the content and discourse of key documents and a series of interviews taken with bank executives. The research finds that the banks' approach to framing and communicating their data governance practices circumscribes their view of potential harms and limits our visibility into how AI is employed. The findings provide insight into potential directions for AI policy and offer a benchmark for future research and regulatory efforts.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my thesis advisor Greg Elmer, Professor, Professional Communication, Toronto Metropolitan University, for his valuable guidance and support in my journey to becoming an academic and completing this thesis. Special thanks to my committee member, Ganaele Langlois, Associate Professor, Communications & Media Studies, York University, for supporting my application to the York & Toronto Metropolitan Joint Graduate Program in Communication & Culture and being a wealth of advice and knowledge throughout my master's program. Special thanks also to my committee member Jonathan Obar Associate Professor, Communications and Media Studies, York University, for generously sharing his deep expertise on data practices and policy.

This endeavor would not have been possible with out the support of my husband, Paul Dillon. Thank you for being such a diligent first reader and for all the nights you prepared and cleaned up after dinner with a smile on your face.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER ONE: INTRODUCTION

What and Why

This thesis explores transparency practices related to the governance and communication of the use of artificial intelligence (AI) in the Canadian banking industry through a case study of Canada's five largest banks. The questions I seek to address are: How are data practices framed and communicated? What beliefs and values are expressed? What are the implications for public trust and for future policy? My research weaves together several areas of inquiry that have fascinated me over the course of my graduate studies. I have worked for decades in digital marketing and have never stopped being interested in what is new in digital media and what might it mean for businesses and for individuals. Graduate studies afforded me the opportunity to broaden my perspective and reflect on what things like big data and AI might mean to society at large – our ways of living and being in the world.

Much of the focus of both academic literature and popular media has been on the negative influence of the tech giants Facebook and Google – from fake news and election interference, to body image and crises of self esteem, to exacerbation of racial and income divides, to the extractive nature of big data marketing and the potential loss of individual agency it represents. But what of all the other sorts of businesses – those not considered tech or digital media companies, but none the less invested in digital persuasion, automation, modeling, big data, algorithms, machine learning, AI…what are they doing and what are the implications positive or negative for individuals and society? After all, companies in many industries employ these techniques in a variety of ways that touch our lives every day, such as customer database segmentation for marketing purposes, automated ecommerce pricing and purchase recommendations, credit

approval, loyalty program incentive and reward customization, and staff recruitment and hiring. This thesis tackles this under explored area of inquiry with a study of the Canadian banking industry.

Graduate studies also allowed me to shift my focus from what is possible from a marketing perspective to what is possible from a policy perspective and consider how AI should be governed. In researching corporate governance in general and AI in particular, transparency is frequently identified as a primary solution. Cries for more transparency abound in the press as well in response to any number of issues related to potential corporate malfeasance or social harm. Pending legislation in Canada and elsewhere is firmly rooted in transparency as a form of governance for AI: Bill C- 27's Artificial Intelligence and Data Act, which had second reading November 2022, requires that "a person who manages the operation of a high-impact (artificial intelligence) system must, in the time and manner that may be prescribed by regulation, *publish on a publicly available website* a plain-language description of the system that includes an explanation of how the system is used; the types of content that it generates and the decisions, recommendations or predictions that it makes" (Parliament of Canada, n.d., italics mine).

But what we mean by transparency and the work transparency does is not at all clear. In fact, this is a rich area of inquiry that has evolved over time. Academics from a wide variety of fields including law and the social sciences have looked at corporate disclosures in terms of how well they achieve transparency: to what degree are they are understood or make clear versus obscure information. Others have taken a critical view of the concept and practices and considered what is being made transparent to whom and to what end – how are social relations and power enacted? Transparency remains a deeply problematic concept and its ability to function as a form of governance is questionable. This thesis unpacks approaches to transparency, taking the position

that a robust perspective that considers both how AI practices are or are not made transparent and how that framing and communication orders social relations is required in order to evaluate the current state of corporate governance of AI and the implications for future policy and regulation. Fundamentally this is an analysis of discourse.

In order to tackle these areas of inquiry - what are companies outside of the tech giants doing with AI, how are they framing and communicating these practices and what are the implications for policy – I have made a case study of Canada's five biggest banks. From largest to smallest, these five banks are: Toronto-Dominion Bank (TD), Royal Bank of Canada (RBC), Bank of Nova Scotia (Scotiabank), Bank of Montreal (BMO) and Canadian Imperial Bank of Commerce (CIBC), as measured by total assets (Statistica, 2021). Given these 5 companies represent 85% of the banking market in Canada (McKinsey, 2019), a study of them is in effect a study of the Canadian banking industry. Although not considered tech companies, the banks all have significant investments in AI. For example, RBC created research center Borealis AI in 2015 (Borealis AI, n.d.), TD purchased AI company Layer 6 in 2018 (Layer AI, n.d.), and in 2020 Scotiabank announced the launch of a global AI platform to deliver insights and advice to customers (Newswire, n.d.).

Canada's five big banks are an ideal focus of study not only due to their size and extent of investment in AI but also due to their unique role in society. Banks are businesses and have an obligation to deliver value to shareholders. In fact, the majority of Canadians are shareholders in Canadian banks, owning shares directly, though mutual funds, and through pensions including the Canada Pension Plan (Canadian Bankers Association, 2023). However, banks are not solely driven by the profit motive. They are the conduit for Canadian monetary policy and act as the federal government's instrument for some social and political policies (Granger, 2017). Banks' obligations to citizens as prescribed by the Bank Act include upholding the right to open a personal bank

account, to cash government cheques free of charge, to receive clear and simple information that's not misleading about products and services and get products and services for which you've provided express consent (Financial Consumer Agency of Canada, 2022). Given that banks must balance profit and public good, their AI practices warrant scrutiny.

Because they perform a critical role in our society, banks are highly regulated. Importantly, much of that regulation is focused on data and computation, particularly since the 1980's with the formation of the Office of the Superintendent of Financial Institutions (OSFI) and the adoption of the international Basel Accords addressing risk management. Risk models, which assess the likelihood of assets increasing or decreasing in value due to market conditions and guide decisions on capital management (pricing, holding, buying, and selling), are subject to extensive requirements under Canada's Bank Act. What might other industries learn from the banking industry with it's strict and long-standing data governance practices and regulations?

There has been some study of the data practices in the financial industry, most notably Pasquale's *The Black Box Society* (2015), several examinations of credit score practices (Campbell-Verduyn et al, 2016; Citron & Pasquale, 2014; Kear,2017; Lauer,2017; McClanahan, 2018), and recent investigations into robo-advisors (Hildebrand & Bergner, 2021; Shanmuganathan, 2020). Most papers examine the impact on individuals or discuss how or why AI could be implemented (Hentzen et al, 2021). There has been very little case study work done, with few papers examining the internal practices of financial companies, and none tackling the Canadian banking industry. Similarly, case study work that examines corporate AI and data practices in the context of transparency are very limited. Most academic literature focusses on what AI transparency practices such as disclosure and explainability could or should look like. Studies that address current practices typically look at data use disclosures in the context of privacy regulation. Few

challenge or problematize the idea of transparency and none address practices in the context of proposed Canadian AI regulation.

A study of how AI is framed and communicated in the Canadian banking industry represents important research at a critical moment in time. New AI governance regulation is pending and with many details still to be fleshed out, now is the right time to question whether the reliance on transparency will protect Canadians from potential harms. Bill C- 27's Artificial Intelligence and Data Act pertains to 'high impact' AI systems which will certainly encompass much of what the banks do given their central role in how citizens participate in the economy. Given the extent of regulation and that fact that the banks are deeply invested in maintaining public trust and managing the narrative of their business and role in society, it can be assumed that the banks' discourse related to AI very likely represents the highest standards of disclosure and attention to risk of harm that can be found in the private sector in Canada ahead of any AI specific legislation. This thesis asks what might be learned from the practices of such a highly regulated, data rich industry, and how might those learnings be applied to other industries – industries whose impact on citizens' wellbeing may not be as profound but are none the less substantial. Research in this area at this moment in time provides a benchmark of practices prior to new regulations and insight into how the banks, other industries, and legislatures might proceed to ensure Canadians realize benefits rather experience harm from the expanding deployment of AI.

In order to arrive at robust findings and meaningful recommendations, this study employs both qualitative and quantitative methods to evaluate the content and discourse of key documents related to the disclosure of AI practices and a series of interviews taken with bank executives. A total of 7 interviews were conducted with executives at all five banks. Interviews were semi structured, with broad questions that allowed the executives speak to their areas of expertise and

reveal their priorities and values. Given the size of the banks and the reality that AI practices and governance involve multiple departments and a wide variety of experts, these cannot be considered complete or definitive representations of the practices of any one bank or the banking industry. Rather, they provide insight on the spectrum of what matters most to the banks and how they are evolving to meet the challenges of governing AI. As happens with research, the process of securing the interviews was in some ways as illuminating as the interviews themselves.

Defining AI

Throughout this thesis I use the term AI for simplicity's sake – not because it's the most accurate (it isn't at all) but because it's the term most used by companies, media, and the government to describe the collection of evolving practices that process data to generate content and make predictions and decisions. While the term has its roots in work done as early as the 1950s that focused on the dream of creating robots or computers that could think like humans, today it typically refers to work done by computers that might also be characterized as 'machine learning', 'deep learning', 'automated decision making', 'predictive analytics', or 'algorithm driven'. For the purpose of this thesis, the term AI will be employed and defined in the sense most often used in the financial industry as the actions and outcomes of algorithms working on big data sets.

These actions are commonly unsupervised machine learning involving pattern recognition with the outcome of creating models and making predictions. An examination of AI must encompass both these aspects: what actions is an algorithm taking to optimize towards which programmed outcomes and what data sets in terms of both content and provenance are employed. The governance of AI includes the governance of data. Importantly, "algorithms are not singular technical objects that enter into many different cultural interactions" (Seaver, p.5) but rather "they

are embedded within complex socio-technical assemblages made up of a heterogeneous set of relations including potentially thousands of individuals, data sets, objects, apparatus, elements, protocols, standards, laws, etc. that frame their development." (Kitchin, p.7). The actions of algorithms are iterative in nature as they "learn" to optimize towards programmed outcomes; goals determined by programmers and business executives and outcomes that can evolve over time.

Because big data is central to the functioning of AI, it is impossible to talk about one without the other. Problems with AI are often viewed as data problems, particularly in the case of bias outcomes such as the case where AI failed to recognize the faces of black women because it was trained on images of white men (Buolamwini & Gebru, 2018). Although it may be aggregated and anonymized, in many cases it is personal data (demographic, behavioural, and transactional) that fuels AI models and predictions (applications like ChatGPT, which uses Natural Language Processing and are trained on text data, or image recognition software are examples of exceptions). Importantly, personal data interacts with AI when models and predictions are applied to individuals (such as the credit limit you are extended, the 'personalized' offers you are given, or the answers provided to you by a chatbot). The entanglement of personal data and AI is an important consideration when evaluating how governance, policy, and transparency practices function.

AI applications in banking

Banks are businesses and as such their primary mandate is delivering shareholder value: profits. Banks employ AI to deliver profits via costs savings, extracting more value out of existing customers, and opening new avenues of revenue. Some applications of AI are specific to the financial industry such as high frequency trading, robo-advisors, credit modeling and fraud detection; while others are utilized by a wide variety of businesses, such as chat bots, sorting employment applicants or targeting advertising. Many purposes are internal to managing the bank such as auditing and document management. Other purposes are aimed at customers such as delivering customer service and growing customer value. The following paragraphs detail the most common ways banks around the world employ AI today.

Banks having been using AI to detect fraud (including identity theft) and money laundering activity since the 1990's. Today, AI runs continuously in real time not only detecting but also evaluating anomalies across transactions and interactions between customers, banks and businesses to ensure fraud is detected and false positives avoided. Marco Mengotto, Financial Services Practice Leader at Dell Technologies, asserts that "Even minor improvements in detection accuracy can significantly lower costs and improve regulatory compliance. Banks have been able to reduce false positives in transactional fraud detection using AI capabilities such as deep learning, computer vision and natural language processing. AI has also helped enhance identity verification in compliance with AML (anti money laundering) and KYC (know your customer identity verification) requirements." (Mengotto, 2023). Banks rely on technology partners to provide the latest AI systems. For example, New York based Socure, who's clients include Wells Fargo and CapitalOne, "uses machine learning and artificial intelligence to analyze an applicant's

online, offline and social data to help clients meet strict KYC conditions". (Gossett, 2023). Scotiabank uses Palo Alto, California based Ayasdi's anti money laundering AI (ibid) and TD uses Nederland company FRISS's "AI-powered fraud risk scoring to better detect suspicious and fraudulent claims during the claims adjudication process" (TD Bank Group, 2022).

Another core function of AI at the banks is market risk management. Risk models that assess the likelihood of assets increasing or decreasing in value due to market conditions have existed for a century (Holton, 2002). These models guide decisions on capital management: pricing, holding, buying, and selling. Market risk modeling has become increasingly more sophisticated in recent decades, pulling in larger amounts of more disparate data, and evolving from statistical analysis to machine learning. For example, BMO has partnered with Riskfuel Analytics to speed up the valuation and risk management of structured derivative transactions, using deep learning to replace previously slow simulators with "very fast neural nets" (BMO, 2021).

The application of AI to market risk management has also enabled the emergence of robo-advising for individual investors. Robo-advisors automate the investment process, recommending and managing (though the buying and selling of funds) an investment portfolio based on investor and market data. Because a robo-advisors replace human financial advisors, banks reduce labour costs, improving profitability, and gain customers (revenue) by offering lower fees and an on demand digital experience. Current Canadian regulation does not permit fully automated robo-advisors as decisioning making must left to a human advising representative who reviews AI generated recommendations (Waschuck & Hamilton, 2022).

AI is also used to support institutional investors. For example, RBC's Aiden trading platform learns from and adapts to changing market conditions. According to Investment Executive, "Aiden uses "reinforcement learning," a form of AI based on behavioural psychology that either rewards

or penalizes an algorithm when it makes a decision." (Collie, 2021). AI also informs 'algorithmic trading", which is also referred to as high frequency trading and passive trading. Select USA estimates that algorithmic trading accounted for up to 73% of US equity trading in 2021 (Mordor Intelligence).

Another form of risk modeling are adjudication models. These predictive models support the judgement of credit worthiness – e.g., should you be extended a loan or mortgage and at what terms? Calibration of adjudication is a critical function for banks as they seek to avoid loss through loans defaults or costly insurance claims. A key data input into credit decisioning models is the credit score, which itself may be generated using AI. Increasingly, models include nonfinancial data. For example, Machine Learning and Deep Learning are used in the calculation of usage-based insurance, which is the "statistical calculation of risk premiums based on data about the customers' behaviors (e.g., lifestyle or driving behavior data)" (Soldatos & Kyriazis, 2022, p.6). Data is collected consensually though apps that monitor driving habits and devices such as fitness trackers.

Predictive modeling is also used for marketing and customer service. Anticipating and capitalizing on customer needs based on a wide variety of data inputs (financial, demographic, and behavioural) from a variety of sources (including from data brokers and social media) drives customer satisfaction and incremental revenue. This work is frequently characterized as 'personalization' and may involved targeted and customized communications and offers. For example, in 2020 Scotiabank employed AI working with multiple data sources including customer data on solvency, liquidity, credit history and external data such as job loss prediction, employment industry and use of payday loans to identify customers at financial risk due to the Covid-19 pandemic. According

to the bank, their proactive outreach and support program improved customer satisfaction and decreased delinquency (Scotiabank, 2021)

Another common application of AI in customer service is the chat bot. Chat bots enable banks to provide on demand customer service and money management tools while reducing labour costs. All five banks in this study have chatbots to support customers. For example, TD leverages US based Kasisto's Conversational Artificial Intelligence (AI) platform to power the bank's mobile app chatbot TD Clari (TD Bank Group, 2019).

AI is also used to automate and realize efficiencies in bank operations. Some of these applications are specific to banks such as automating the loan approval process. Many are not specific to banks and may be found in many companies in many industries. One common application is Intelligent Document Processing (IDP) "based on artificial intelligence (AI) subsets: machine learning, deep learning, natural language processing (NLP), computer vision, and optical character recognition (OCR)" (Jaggi, 2023). Banks use IDP to manage contracts, classify mortgage requests, and process cheques (ibid). AI is also used in the hiring process at some banks. HireVue AI is used by Goldman Sachs, JP Morgan, and Morgan Stanley (CFI Team, 2022). HireVue uses machine learning algorithms that analyze data from eye and body movements, facial expressions, and voice to the predict future job performance of candidates (ibid).

Like all businesses, the banks use AI to increase revenue and profitability. AI is employed to reduce loan default risks, avoid the costs that fraud incur, increase customer value with additional sales and loyalty, and cut labour expense and errors through automation. The 'complex socio-technical assemblage' that these activities are part of include various functions within the banks (such as executives, programmers, and analysts), third parties (such as regulators, AI development companies, customers), tools (various dashboards and software) and data sources (such as

transactional, behavioural, textual). Increasingly, data sources extend beyond personal financial information and data is sourced from and shared with companies outside the banks.

The regulatory environment

While the Canadian banking industry is heavily regulated, there is no one set or source of regulations to address the use of AI. "The current regulatory landscape governing the use of AI by in the financial services industry is a broad patchwork of laws and regulations" (Waschuck & Hamilton, 2022). Regulations impacting the use of AI not specific to the banking industry include The Personal Information Protection and Electronic Documents Act (PIPEDA), the Canadian Charter of Rights and Freedoms, and the Canadian Human Rights Act. These regulations address outcomes, such as fairness or privacy protection, that are required regardless of whether or not AI is involved. AI specific legislation in Canada is pending. Bill C- 27 which had second reading in the House of Commons April 2023 and includes the Artificial Intelligence and Data Act with AI specific regulations such requirements for the anonymization of personal data, implementation of harm mitigation measures, and disclosures about the use of AI. These policy initiatives build on our current privacy and data governance law. All these acts and charters lean on transparency as governance, with accountability as a result of either disclosures required of companies or complaints made by the public.

In the case of the former for example, we have public reporting requirements to the Privacy Commissioner when privacy breaches occur (e.g., data leaks) with fines for noncompliance. This type of disclosure ensures individual harms are addressed (such as financial reparations to affected individuals) and creates awareness and knowledge about causes and solutions (for example from a privacy commissioner investigation and report). The costs associated with data leaks made

public provide incentive for good governance, for example, a 2018 leak of data on 113,000 customers at BMO was estimated to have cost the bank as much as $28 million covering fraudulent transactions, a class action lawsuit, credit monitoring and identity protection (Solomon, 2021).

The Artificial Intelligence and Data Act takes a very similar approach to PIPEDA, requiring disclosures to the public in the form of notices online and disclosures to government. Online notice is "a plain-language description of the system that includes an explanation of how the system is used; the types of content that it generates and the decisions, recommendations or predictions that it makes" (Parliament of Canada, n.d.). The act proposes the establishment of an "AI and Data Commissioner to support the Minister of Innovation, Science and Industry in fulfilling ministerial responsibilities under the Act, including by monitoring company compliance, ordering third-party audits, and sharing information with other regulators and enforcers as appropriate" (Government of Canada, 2023). It remains to be seen whether audits will be proactive or only as a result of complaints made, as is the case with the Privacy Commission. It is a risk-based approach, "protecting Canadians by ensuring high-impact AI systems are developed and deployed in a way that identifies, assesses and mitigates the risks of harm and bias" (ibid). However, concerns have been voiced regarding the ability of the Act to effectively govern AI given the conflict of interest inherent in an AI and Data Commissioner reporting into a ministry tasked with promoting Canada's tech sector (Globe Editorial Board, 2023).

Overseeing policy, regulation and supervision of Canada's financial sector are the Department of Finance Canada, the Financial Consumer Agency of Canada (FCAC), the Office of the Superintendent of Financial Institutions (OSFI), the Bank of Canada, and the Canada Deposit Insurance Corporation (CDIC). In addition to requiring a variety of transparency practices, these organizations stipulate governance practices, such as the OFSI requirements around board of

director composition and functions. Financial institutions are subject to direct oversight to ensure requirements are met. For example, the OFSI requires a variety of disclosures and reviews "information obtained from statutory filings, financial reporting requirements and management reporting to the board" (OSFI, 2014) in order to determine if a financial institution is meeting requirements. It has the power to intervene if they are not. Expert public bodies, not individual citizens, ensure the good governance of banks.

At present, the governance of the development and deployment of AI and it associated models, data sets and algorithms is left to individual companies. The OSFI's Guideline E-23 specifically places the onus on FIs to develop their own sets of policies and procedures ''in order to identify, assess, manage, and control the risks inherent in any model". Note that this guidance refers to "any model" not AI specifically. The OSFI provides supervision in the form of auditing models every few years, however only risk and adjudication models are audited, other models (which may employ AI) such as marketing propensity models (e.g., likelihood of a client to open a TFSA account) are not subject to external auditing. In a recently published report on responsible AI, the OFSI reiterated its commitment to the principle of explainability (OFSI, 2023) – a transparency practice enabling the back and its customers to provide an explanation of how a model arrived at a recommendation. This report is a discussion document ahead of new regulations. AI specific regulations are in development with implementation targeted for June 2024 (OFSI, 2022).

The transparency practices we see in both current and proposed legislation involve disclosures to the public and to regulatory bodies. But are these disclosures effective in regulating AI? Do they protect us from all harms? We also see managed visibilities (Flyverbom, 2016; Stohl et.al, 2016) at work – the banks employ the term AI to encompass a wide variety of activities which obscures just how and to what end algorithms are working on big data sets. How do ways in which the banks

communicate about AI impact our understanding of benefits and harms? What can we learn about the banks' data and AI governance practices and the ways in which they are communicated? How might that knowledge inform policy?

I contend that the only way we can begin to answer these questions is to first problematize transparency. What is transparency and what works does it do? Situating how AI and data practices are framed and communicated as transparency practices provides a foundation for understanding what beliefs and values are held about AI and AI governance. It through this analysis of the transparency discourses at the banks, both written and in the interviews, that we can begin to evaluate AI governance policy. Problematizing transparency enables us to see *how* regulation does or does not work. Second, we need to enumerate and understand the potential harms associated with using AI. A comprehensive view of all the issues provides a basis of comparison as bank practices and proposed legislation are interrogated. Understanding harm enables us to see *what* we are and are not protected from.

In the following pages I will walk through a literature review that examines why we call for transparency, what we might mean when we do, and in that context what research already exists about corporate transparency practices in general and AI and banking practices specifically. Following that I provide an exploration of what academic literature has to say about the potential individual and social harms that may arise from deploying AI in general and within the financial industry. I will then take you through the methods used for the document and interview analyses and the findings for each. This will be followed by a discussion of how the finding address my research questions and a conclusion that will include implications for AI governance and policy as well for future research.

CHAPTER 2: LITERATURE REVIEW

Problematizing Transparency

Talk about the need for transparency is everywhere. A search of "transparency + banks" on Google News returns more than 92 million results with headlines like "The Bank of Canada still lags in transparency" (Schembri & Globerman, 2023) and "Good governance, transparency key to revive economy" (TBS Report, 2023). As discussed, much of our current and proposed legislation rely on transparency practices. But what do we mean by transparency? And what is achieved by transparency practices? This section of the literature review addresses these questions in order to provide the foundation for addressing the questions this thesis seeks to answer: How are data practices framed and communicated? What beliefs and values are expressed? What are the implications for public trust and for future policy?

For such a commonly used term, transparency as a metaphorical concept is remarkably resistant to definition. It generally understood in the context of organizations to mean the disclosure of information to an audience so that they may see into the actions, practices and/or policies of that organization. It is an act of communication. The *assumption* is that this disclosure will lead to accountability and good governance on the part of the organization and the opportunity to make better decisions on the part of the audience. The key word is assumption, "a thing that is accepted as true or as certain to happen, without proof." (Oxford Dictionary, n.d.). The outcomes of transparency practices against their stated aims are seldom measured and when they are, results are mixed at best (Cucciniello et al, 2017; Etzioni, 2010). Transparency practices are founded on beliefs. One content analysis of 150 academic journals discussing transparency found 18 different definitions and offered this consolidated definition "Transparency is the *perceived* quality of

intentionally shared information from a sender." (Schnackenberg & Tomlinson, 2016, emphasis mine). Transparency practices have an "affective dimension, tied up with a fear of secrets, the *feeling* that seeing something may lead to control over it, (Ananny p. 975, emphasis in the original). And yet despite the reality of assumptions, perceptions and feelings, transparency practices and disclosures are characterized as fact or truth.

There is a belief in the achievability and neutrality of transparency, that is, a perfect or ideal state of seeing things as they really are. Emmanuel Alloa calls it a "magical concept",

> "… it boasts broadness (covering large domains and having multiple, overlapping, and sometimes conflicting definitions), normative attractiveness (this can be tied back its positive connotation), implication of consensus (diluting, obscuring, or even denying traditional social science concerns with conflicting interests and logics), and last but not least global marketability (being well known as well as fashionable, among the most diverse audiences). In other words: it is extremely hard to be against transparency." (Alloa, 2019, p.29)

Taking up the idea that is hard to be against transparency, we see it also identified as a "Major Good" (Etazioni, 2018) and a "hallmark of organizational legitimacy" (Flyverbom, 2019, p. 85). Transparency has been referred to an "illusion" (Hong, 2020) and an "ideal" (Flyverbom, 2019). Transparency has also been characterized as a myth:

> "Although science, philosophy and social behaviour, as we have seen, frequently defy the notion of unqualified transparency, including the possibility of self-transparency, its value is nonetheless continuously reproduced again and again in political, corporate and popular discourse… transparency is repeatedly activated, across organizations and situations, as an

> indisputable description of how society and its institutions ought to develop and function…As an authoritative belief in the possibility of ever-increasing insight and clarity – and thus as a precondition for a rational, efficient and just society – transparency is arguably one of the foundational myths of modernity" (Christensen & Cornelissen, 2015, p.137)

Transparency is not simply a myth in the sense of "a widely held but false belief or idea" (Oxford Dictionary, n.d.), although many contend this is so and many articles have been written demonstrating that true transparency is an impossible ideal (Ananny & Crawford, 2018; Etzioni, 2019; Bearman & Ajjawi, 2018). Transparency practices are also myths in the sense that they describe the world the way we believe it to be: "myth presents itself as an authoritative, factual account, no matter how much the narrated events are at variance with natural law or ordinary experience". (Encyclopædia Britannica, n.d.). Transparency practices are *stories* we tell, grounded in beliefs and values, about how the world works.

Numerous aspirations and values have come to be associated with the term transparency, including defeating corruption, ensuring accountability, and creating trust. When it comes to discussing organizational transparency practices, these 'powers' of transparency are encapsulated in Brandeis' oft used quote "Sunlight is said to be the best of disinfectants; electric light the most efficient policeman". (Brandeis, 1913) Also important is the idea of disclosing information to achieve fairness or to reduce asymmetry/rebalance power (Alloa, 2019; Forssbæck & Oxelheim, 2014; Heald, 2016). Transparency is able to embody these aspirations and values as a result of the attendant belief in the rational actor and the idea that 'if I have factual information, I will make better decisions' (Hong, 2020, p. 38; Etzioni, 2019, p. 190; Flyverbom, 2019, p.13).

The idea of the rational actor comes with its own set of assumptions: that I have the interest, time, and ability to scrutinize the information, that I am empowered to make choices as a result of being given information and that I am willing to make those choices. These assumptions support the use of transparency as regulation – which is to say transparency is not only regulated, in that it may be required by law, but disclosure itself is believed to be sufficient to regulate behaviour. The burden is placed on the individual to know and judge – assuming people "have ways of discussing and debating the significance of what they are seeing" (Ananny & Crawford, 2018, p.980) and that "individual choice (is) the atomic unit of ethical behaviour (Hong, 2020, p.192).

In reality there is abundant research and unlimited examples of how people do not access information or exercise rational choice. In the context of corporate transparency practices, for example, people seldom engage with or understand privacy policies, nor do they modify their behavior when exposed to them (Obar & Oeldorf-Hirsch, 2020; Turow et al, 2019; Rice & Bogdanov, 2019). This is not to say that people do not care how their data is used (and possibly used against them) regardless of how they behave. It may be that they believe they are being afforded greater protection then they are given the "designed obscurity" of privacy notices (Martin, K., 2015) or that they lack awareness about the extent of data being collected and the uses it is being put to (Hitlin, & Rainie, 2019).

The magical myth of transparency also assumes that we can get, or at least should be attempting to get information that is accurate, complete and without bias. In fact, we may find ourselves in a "flood of information, drowning us in a sea of unstructured and boundless data that overwhelms our cognitive and interpretive capabilities, and hence renders information meaningless or confusing and opaque." (Stohl et.al., 2016).

The study of transparency typically puts information at the center: what is being disclosed and how? Albu & Flyverbom note in their literature review of 129 articles and book chapters on organizational transparency practices in research areas such as management and organization studies, the humanities, economics, sociology, psychology, and government law that "that transparency research can be divided into (a) approaches with a focus on information provision and accuracy, and (b) perspectives that stress the importance of social, communicative processes, and the complications arising from transparency projects (Albu & Flyverbom, 2019). Category (a) focuses on the role of information disclosure, which the authors label the "Verifiability Approach" as these papers "consider transparency to be a matter of demonstrating via disclosure that something is true, accurate, or justified" (ib id, p.283). Similarly, Schanckenberg & Tomlinson's review of 150 research papers on organizational transparency identifies the field's primary focus as information disclosure, categorized as disclosure (timeliness, accessibility), clarity (intelligibility, interpretability) and accuracy (reliability, replicability) (Schanckenberg & Tomlinson's, 2016). This focus on information tends reduces transparency practices to a linear model of communication along the lines of *A Mathematical Theory of Communication* (Shannon & Weaver, 1948) where we have a transmitter (the organization), the signal (the information to be disclosed), noise (factors that must be managed to ensure the information is clear and accurate) and the receiver (the audience which may be the public, a consumer, an expert involved in oversight or a partner to the organization).

This framework has been identified as an oversimplification, where "senders are compliant information providers, messages are clear and self-evident, and receivers are consistently interested and involved" (Christensen & Cheney, 2015, p.73) and criticized for ignoring "the multiple roles that communication plays in establishing complex relationships among the parties

to the communicative act" (Fenster, 2015, p.254). Transmitting information is not the same as imparting meaning. None the less, this framework's extensive employment in organizational transparency studies is evidence of its power in articulating the myth of transparency – it provides an easily understood narrative arc. By putting information at the center of the story, this approach supports the belief that the more information we have, the more insight we have (Flyverbom, 2019, p.86). By treating transparency *as* information – a thing in and of itself - versus what we want out of a practice of transparency, such as greater trust or a rebalance of power, this approach can lead to transparency showing up as an end rather than a means in practice. The artifact – a report or policy – is seen not as a representation of reality but truth itself (Christensen & Cheney, 2015). Belief in the power of information supports the idea that it can function as regulation.

A more critical perspective has emerged in recent years that decentres information in order to address the contradictions and complication within transparency practices. Characterized as "performative transparency" (Albu & Flyverbom, 2019) and "visibility management' (Flyverbom, 2016; Stohl et.al, 2016), this approach considers the role of a variety of actors, both human and technological, play in mediating both the disclosure and representation of information as well as its obfuscation, along with the resulting effects, intended or otherwise. Transparency practices are performative in that they are a form of social ordering that shape our conduct and produces relations and boundaries (ibid, 2019): the effects are not simply the stated intentions (e.g., informing the public). In this respect, transparency practices can be understood as a form of power and control: "transparency always involves choices, asymmetries, and divisions – who can observe whom, which activities are opened up and which kept closed and which objects and processes are subjected to transparency efforts and which are not" (ibid, p.54). Transparency practices proport to be a form of control of the organization (e.g., a regulatory requirement to disclose various forms

of information), but they also represent an opportunity for the organization to exercise control in terms of the selection, type, presentation, and legibility of that information (Flyverbom et al, 2015). Numerous authors have pointed out the ways in which transparency practices can achieve the opposite of what they intend. For example, cases where "so much information is visible that unimportant pieces of information will take so much time and effort to sift through that receivers will be distracted from the central information the actor wishes to conceal." (Stohl et. al., 2016).

Shifting the focus from information to actors also enables deeper reflection on the role technology plays in the mediation and representation of information. Technology plays a role throughout the process of producing visibility, from the inscription and storage of data through to its selection and classification (Stohl et. al., 2016). The disclosure of data is also mediated by technology in ways that can either reduce or improve accessibility and comprehensibility. Consider how consent to cookies is managed when navigating online: depending on the website, Canadians may be notified via a privacy policy that must be accessed through a link in small print at the bottom of a page; by a banner that announces by using the site that you accept cookies; or, modeled after the current EU model under GDPR, a pop up that requires you to select what you agree cookies can be used for that can be several pages deep each with its own list of things for you to consent to. An evaluation of who is controlling the information being disclosed, how and with what effect on the conduct and relationships between human and technological actors is a critical aspect of understanding organizational transparency practices.

This review of the concept of transparency and the ways in which transparency practices may be described or understood reveals complexity and contradiction. Transparency practices are positioned as straight forward disclosures of information, but they can hide as much as they reveal. Transparency practices ask us to believe that information is a complete and accurate reflection of

reality and its presentation is synonymous with trustworthiness and truth when in fact it is mediated through selection, technology, and language. Transparency practices are used to empower us to judge for ourselves information that we may not have the power to understand or act on. This thesis contributes to the nascent body of literature on performative transparency by exploring the values and purposes that can be understood by bank disclosures as opposed to simply evaluating the quality or validity of the disclosures themselves.

"inward" transparency practices related to corporate use of AI

Call for transparency around data and AI are calls for "inward" transparency practices: allowing those outside the organization to see what is happening inside the organization (Heald, 2006). While numerous academics have called for transparency – from Pasquale's exhortation for the disclosure and auditing of algorithms in The Black Box Society (2015) to Noble's call for greater transparency to "slow down the automation of our worst impulses" in Algorithms of Oppression (2018, p.145) - academic literature specifically addressing transparency practices connected to AI are extremely limited. This not surprising given the current state of AI regulation. GDRP (General Data Protection Regulation) with its requirement for disclosures related to the use of data only came into effect in 2018 and the UE's new Artificial Intelligence Act is still going through amendments as of January 2023. The United States lacks any comprehensive regulation. Individual states having various legislation pending and only California has enacted law similar to GDPR. In Canada, Bill C-27, which includes the Artificial Intelligence and Data Act, just had second reading April 2023.

Most academic literature focusses on what AI transparency practices such as disclosure and explainability could or should look like. These include practical and applied methodologies

(Herden et al., 2021; Ibiricu & van de Made, 2020; Lobschat et al., 2021; Saltz & Dewar, 2019; Yeung et al., 2020), and critical theory-based frameworks (Ananny, 2016; Buhmann et al., 2020; and Park et al., 2018). These methodologies and frameworks consider the governance of AI assemblages and how accountability can be achieved across technical, institutional, and individual actors and stages of development and deployment. Transparency is typically situated as a practice to be considered at different points in time and places in the assemblage, such as data providence (Herden et al., 2021), codes of conduct (Herden et al., 2021), intended use or function (Buhmann et al., 2020; Ibiricu & van de Made, 2020; Yeung et al., 2020), prototyping (Yeung et al., 2020) and outcomes (Buhmann et al., 2020; Saltz & Dewar, 2019; Yeung et al., 2020).

Transparency is often viewed as analogous to explainability in AI governance (Ibiricu & van de Made, 2020; Lobschat et al., 2021; Saltz & Dewar, 2019). This is the perspective taken by a recent legal paper that looks specifically at AI governance in Canadian banking. Payette and Torrie contend that legislation and guidelines already in place to protect Canadians, such as the Canadian Human Rights Act, Office of the Superintendent of Financial Institutions (OSFI) guidelines and PIPEDA, also apply to the use of AI, limiting the need for additional specific AI legislation. (2020). With regard to transparency requirements, the authors acknowledge that AI models operate at a new level of sophistication relative to past models employed by banks, presenting challenges to explainability. They suggest that financial institutions "may deliberately choose to use types of AI that are less opaque based on regulatory requirements, or other legal and ethical obligations" (ibid, p.11).

A few studies have moved beyond the theoretical to examine actual corporate governance practices related to AI. Ibabez & Olmeda spoke with 22 executives at companies in Spain for their paper "Operationalising AI ethics: how are companies bridging the gap between practice and

principles?" (2022) which included a discussion of explainability (which while not characterized as such by the authors is a type of transparency practice). They found that companies lack formal procedures and guidelines and that explainability is perceived as challenging and complex. Stahl et al employed a case study approach, interviewing 42 people at 10 companies across 5 countries for their paper "Organisational responses to the ethical issues of artificial intelligence" (2021). Transparency is situated as a competing good in their findings. On the one hand companies worry about protecting intellectual property and some feared people "gaming the system" if provided with information, while on the other hand, other interviewees felt that codes of conducts and general principals should be made public. These two studies form the basis of a comparison of and benchmark for the current state of corporate governance of AI that this study will in part leverage and add to by looking at the practices in the Canadian banking industry.

Recent academic research specifically on inward corporate transparency practices largely focus on the analysis of key artifacts of transparency and disclosure. These include discourse analysis of annual reports, which while not explicitly framed as transparency practices clearly demonstrate that visibility management (Flyverbom, 2016; Stohl et.al, 2016) in terms of what is disclosed (and not) and how (Chakrabarty et al, 2018; Qian, 2020). For example, a study of thousands of annual reports by Chakrabarty et al showed that managers with higher risk incentives publish less readable disclosures (ibid). Similarly, there has been extensive analysis of the ways in which corporate social responsibility documents manage disclosures and work to position companies positively while obscuring issues, particularly those related to environmental sustainability activities (Jaworska, 2018: Martins et al, 2021). However, none of these studies specifically examine disclosures related to the use of data or AI.

Another popular subject is privacy policies as these are "relied upon to inform individuals' decisions about the collection, processing, sharing, and reuse of their personal information" (Bruening & Culan, 2016. p.517). While most of these do not typically situate privacy policies as a transparency practice per se, they do focus on accuracy and understandability of the information disclosed, including readability (Das et al, 2018; Fowler et al 2020; Li et al 2012; Obar, 2022; Zang et al 2020), compliance to stated practices (Brandtzaeg et al, 2019, Huckvale et al, 2019.) and public interaction with or understanding of privacy policies (Obar & Oeldorf-Hirsch, 2020; Turow et al, 2019; Rice & Bogdanov, 2019). In the third Data Privacy Transparency of Canadian Internet Carriers report, Obar rates stated data disclosure practices against 10 criteria based on the "spirit of PIPEDA's openness principle" (Obar, 2019, p.15), giving the top ten retail internet carriers scores that ranged from 2.5 to 8 out of 10. All these papers point out the shortcomings of privacy policies: that they are difficult to understand, often incomplete or incorrect, and are frequently skipped over by consumers. These papers demonstrate that privacy policies fail as transparency practices intended to enable meaningful consent or individual choice and control. Privacy policies are a form of manage visibility. They may meet regulatory requirements in terms of information to be disclosed, but not the spirit of the regulation. They are in fact designed to be ignored, facilitating the collection of personal data and obscuring data practices.

Transparency in the form of required disclosures to consumers fail as a way to regulate data use practices under today's privacy legislation. Research shows that actual data practices often do not meet the terms set out in privacy policies or required in regulation. Huckvale et al assessed the data transmission behavior of 36 health apps available in the US and Australia. They found that while only 23 apps had privacy policies that stated data would be transmitted to a third party, transmission was actually detected in 33 apps (Huckvale et al.). Similarly, studies by Brandtzaeg

et al (2019), Grundy et al (2019) and Krych, & McDaniel, (2021) provide evidence of data transmission, including personal information, and tracking practices not disclosed in privacy policies.

Studies on data disclosure practices focus on personal data and privacy. The collection of personal data is essential to building the big data sets used in AI applications and disclosing with whom data shared and for what purpose is part of current privacy regulations. However, AI largely uses anonymized data which, being no longer personal, is not subject to privacy law. The AI disclosure requirements pending in Canada focus on the use and outputs of AI systems. Findings showing that current privacy disclosures are at best ineffective and at worst inaccurate and misleading are likely indicative of what we might expect following new legislation. However, AI transparency practices must emerge as a unique area of study.

There is considerable literature in the private sector about AI and banking. Much of it is generated by consulting firms and focused on the why and how of AI in aid of securing consulting contracts (Biswas et al., 2020: Galaski, 2021) Consulting firm Evident Insights, who's stated mission is "to bring transparency to the adoption of artificial intelligence in business by creating the global standard benchmark of AI maturity" (Evident Insights, n.d.) recently published a report on the AI maturity of 23 of the largest banks in North America and Europe (Mousavizadeh & Ayles, 2023). The report's benchmark is derived from publicly available data and scores banks on their talent, innovation, leadership, and transparency. Transparency is measured by the extent to which the banks publicly communicate their responsible AI activities (e.g., though the publication of ethical principles) and make visible the controls they have in place (e.g., through the announcement of dedicated responsible AI or AI risk management roles). The measure of leadership includes "the existence of a public AI narrative across group-level investor materials, press releases and media"

(ibid, p.9). The report ranks RBC second and TD banks sixth out of the 23 banks studied, stating "this relative success is driven by strong performances on Transparency and Leadership" (ibid, p.12). This is a study of the extent to which the banks are managing visibility of their AI practices.

My research uncovered only one peer reviewed academic study specifically focused on corporate AI disclosures (versus data collection and use). Wulf and Siezov (2022) examined the effectiveness of AI disclosures (annual reports and privacy policies) mandated by GDRP by surveying 835 people regarding their expectations of data disclosures and then conducting a content analysis of AI disclosures from 100 companies and organizations. They found that while 57% of disclosures meet current GDRP requirements only 18% of those surveyed believe disclosures met their expectations of being told when an algorithm is in use, what its basic logic is, and what personal data it employs. This study reveals a significant gap between GDRP, which already sets a higher bar than current US and Canadian regulation, and public expectations of AI disclosures. While establishing a benchmark of GDRP compliance and offering insight into how compliance can be improved and regulations evolved, this study does not challenge the underlying assumptions of transparency.

Three studies that interrogate transparency practices in Fintech from a performative perspective and look at how disclosures enact power relations and create new avenues of financialization are Crain's "The limits of transparency: Data brokers and commodification." (2018), Bourne's "Fintech's Transparency Publicity Nexus: Value cocreation through transparency discourses in business-to-business marketing" (2020) and Zook and Spangler's "A Crisis of Data? Transparency Practices and Infrastructures of Value in Data Broker Platforms." (2023). These studies explore practices that have emerged as a result of the data sharing and open banking regulations that followed the 2008 global financial crisis. Fintech companies adopted the discourse of transparency

as incumbents were cast as opaque, gaining legitimacy and opening new avenues of revenue. Data transparency practices initially positioned as an opportunity to empower investors and avoid future crisis – providing Brandeis' 'sunlight' and 'disinfectant' – transformed into technological transparency: the pursuit of joining disparate data sets and perfecting data interoperability with the idealized goal of seeing the market perfectly. Data made transparent (at accessible but incomprehensible volumes) was managed, sorted, and visualized (made legible) by data brokers and commodified in ways which demonstrate that "transparency functions as a discursive construction that creates suitable conditions for the manufacture and extraction of data as an asset" (Zook & Spangler, 2023, p.123). Focusing on transparency as a solution to the crisis meant that "policy responses need not focus on controlling greed, simplifying debt instruments, or implementing policies that value the health of people over the health of markets." (Ibid, p.112). These studies demonstrate how transparency practices are a form of social ordering that can subvert stated goals of consumer empowerment and further strengthen a regime of collecting and monetising personal data.

There is a great deal of academic literature that circles around corporate transparency practices and AI but very little that addresses this topic directly or robustly and none look at the Canadian banking industry. Many articles focus on what could or should be done in terms of governance or regulation of AI, not what is being done. Those that do focus on corporate transparency practices are not focused on AI (apart from Wulf and Siezov's study) or banking but instead evaluate data disclosure and practices in the context of privacy. Importantly most studies on corporate transparency practices, including Wulf & Siezov's, focus on the degree to which transparency is achieved, analysing what is being made transparent. Very few studies explore the broader implications or effects of transparency practices or problematize the concept itself.

This thesis serves to address these gaps and contribute to the nascent body of literature on transparency practices that address AI in several ways. First it will provide holistic analysis on transparency practices: looking at not just if transparency is achieved or what transparency does, but rather employing both the 'verifiability' and 'performative' approaches. Second, this research will provide new insight into corporate practices related to AI through a multi model case study approach combining the analysis of documents along with interviews with company executives. Finally, in focusing on the Canadian banking industry ahead of new pending legislation on AI disclosures, this thesis serves as a benchmark from which evolving practices can be evaluated and understood.

The potential for harm

While this thesis will not add to our understanding of the harms that may results from the deployment of AI, it will evaluate how and to what degree current bank governance practices and proposed legislation address harms. This section of the literature review explores the many types of harms that have been identified by academics over the past six years. It should be noted that the intention of this review of potential harms is not to discount the tremendous opportunities and advantages the deployment of AI may bring to individuals and society, but rather to understand where regulation may be needed to ensure those advantages are realized safely and equitably.

The societal and individual harms activities associated with data, algorithms and artificial intelligence have been extensively researched and discussed. Documentaries like The Social Dilemma (2020) highlight the dangers of addiction and behavior modification while academics like Shoshana Zuboff (2019), Cathy O'Neil (2016) and Safiya Umoja Noble (2018) warn of pervasive exploitation and control. Canada's proposed Artificial Intelligence and Data act defines

harm broadly as “physical or psychological harm to an individual; damage to an individual’s property; or economic loss to an individual” (Parliament of Canada, n.d.). Specific harms include cybercrime, privacy and data security, fake news and manipulation of public opinion, social engineering, labour disruption and job loss, discrimination and exclusion, and environmental harm (Herden et al., 2021). All these harms with the exception perhaps of fake news and manipulation of public opinion have the potential to be realized in the Canadian banking industry.

Despite the breath of potential harms, academic and legal scholars have been largely concerned with bias and fairness in the financial sector. Numerous studies have demonstrated that many applications of AI have been built on bias data sets and result in bias outcomes. Well known cases include facial recognition software trained primarily on white faces that fails to correctly identify black faces (Buolamwini & Gebru, 2018), and the alarms raised about policing applications founded on historical racially bias data (Heaven, 2020). AI in the recruitment process has also been subject to criticism. Drage & Mackereth note that tools evaluating gestures, voice and eye movements in interviews “naturalize attributes as biological universals, obscuring how they might be learned as well as how they are always culturally contingent” (2022, p.89).

AI can output a bias result even when variables such as gender or race have been excluded from initial data sets as AI systems create proxies and can readily fill in missing data. Subsequent machine learning can result in biased correlations and inferences. Payette and Torrie offer this financial industry example: “auto insurance risk assessment might determine that accidents are more likely in certain neighbourhoods. If racial minorities tend to reside more in these areas, the AI model may infer that these minorities are more likely to be in accidents.” (2020, p.10). The Financial Consumer Agency of Canada notes in its 2021 -2026 strategic plan: “Use of artificial intelligence and algorithms that can negatively affect access to appropriate products or services

(e.g., digital profiling that disadvantages certain groups)" are a risk to consumer protection (Financial Consumer Agency of Canada, 2021)

Bias in credit scoring has long been a subject of academic criticism. The modern credit score, a single 3-digit number representing a person's credit worthiness, emerged in 1989, replacing individual lender and small credit bureau judgement. This standardize approach was perceived as being more scientific, fair, and free of bias. (Lauer, 2017). In Canada two credit bureaus, Equifax and TransUnion, produce credit scores for Canadians. According to the Consumer Reporting Act of Canada, credit scores are to be comprised of the following data points: name, age, occupation, place of residence, previous places of residence, marital status, spouse's name and age, number of dependants, particulars of education or professional qualifications, places of employment, previous places of employment, estimated income, paying habits, outstanding debt obligations, cost of living obligations and assets. Importantly, while banks access and consider an individual's credit score when assessing worthiness for a loan or mortgage, the score is not the only consideration at play. Banks can access additional data points and employ AI in assessing extension of credit in order to further mitigate risk and save costs (predicting who may be likely to default on debt or be perpetrating fraud) or uncover new revenue opportunities (potential customers that may be overlooked based on an Equifax or TransUnion score alone). "AI can analyze additional unstructured and semi-structured data drawn from social media, text messages, and search engines usage to complement traditional credit-scoring methods, providing for a more nuanced view of credit quality" (Caron, M.S., 2019). While the introduction of additional data sets and the application of machine learning opens up opportunities to extend credit to those who otherwise would not receive it, it also increases potential for bias. Robin Nun cautions "as the lending industry digitizes and moves toward "alternative lending" (i.e., considering non-traditional

creditworthiness factors, including behavioral data), financial institutions must balance the innovation of AI with the substantial risk that machine learning could result in disparate impacts on minority populations." (2020, p.182).

While harms associated with social engineering and behaviour modification are most frequently attributed to social media, several authors have explored how the ever-increasing financialization of all aspects of life that AI and big data enable exasperate information asymmetries, reduce freedom of choice, impact behavior and create new social relations. Kear provides a simple example of behaviour modification in the story of a women who would prefer to use cash feels compelled to use credit in order to build a credit score, noting she and others "recognized that algorithmic identities are only loosely coupled with self-identity, but that any gap between them could redound to their disadvantage." (2017, p. 355). In Re-Engineering Humanity, Frischmann and Selinger consider the practice of nudging (a 'behavioural economics' practice in the language of fintech) and ask "does the change induced by the constructed environment constitute a reduction or addition in human capability? Is it diminishing or empowering?" (2018, p.385). Zubof provides a grim answer: the goal is "to produce behaviour that reliably, definitively, and certainly leads to desired commercial results" (2019, p.240), creating a new collective order that robs individuals of agency and sovereignty and enables "concentrations of wealth, knowledge, and power unprecedented in human history" (ibid, p.7). The Financial Consumer Agency of Canada recognizes the "use of gamification and behavioural designs that encourage impulsive financial decision-making and access to high-cost, short-term credit" as risks to consumer protection. (FCAC, 2021). In response, FCAC regulation has evolved to recognize and harness the power of nudging for the public's benefit: "As of June 30, 2022, banks will be required to send new electronic alerts to their customers. The alerts are part of the new and enhanced measures to protect

consumers in Canada's Financial Consumer Protection Framework" (Canada, 2022) and include notification of low balance and upcoming bill payments.

Recent developments in online stock trading supported by AI and machine learning (via platforms that employ robo-investing, predictive modeling, speed trading and other emerging applications) provide an example of both the potential for individual agency AI affords and consolidation of power that restricts it. Online trading is a financial service positioned as empowering individuals currently being heavily marketed to young adults as an easy way to build to build wealth. Commercials like "TD Easy Trade: Becoming an Investor" suggest that no experience or knowledge is required (2022) and open up a new revenue stream for the banks losing out on mortgages that will not materialize as so many are shut out of the housing market. However, when individual investors began to drive up GameStop share prices in 2021, trading was not just paused on the NTSE (an established practice to address volatility) but subsequently several trading platforms, including TD Ameritrade, Charles Schwab, and Robinhood, restricted retail (individual) buying - but not institutional buying. This lead to extensive outrage - "Robinhood canceled stock orders on #gme #amc #NOK etc.... There should be a class action lawsuit. I thought we had a free market. So Wall Street is OK with me losing hundreds of dollars, so that rich investors can't be called out on their risks" (Fitzgerald, 2021) - along with lawsuits and a government inquiry. This power struggle clearly shows the material limitations that can be quickly placed on individuals in a platform environment.

AI and data practices also exact a toll on our planet. While these are not particular to the financial industry, it like all other industries, is complicit in the harms wrought. As Crawford notes in *The Atlas of AI*, "it takes a gargantuan amount of energy to run the computational infrastructures of Amazon Web Services or Microsoft's Azure, and the carbon footprint of AI systems that run on

those platforms is growing (2021, p. 44). Mining for the rare minerals needed for computing has created environmental and human disasters in places like the Congo, the source of 70% of the world's cobalt (Statistica, 2023), which is used in the AI we all carry in our pockets, our mobile phones. While we imagine that AI is invisible and 'the cloud' as clean and white, "artificial intelligence is both embodied and material" (Crawford, 2021, p. 14) and has a very real impact on the planet.

AI also disrupts labour through job displacement, outsourcing work to customers, and exploitation. A recent study estimates that almost 20% of workers may see at least 50% of their tasks impacted just by the introduction of ChatGPT and other large language model AIs alone (Eloundou et al., 2023). Given that new technologies have been making some jobs obsolete while creating new ones for decades, this is often not thought about as a harm but as just the way things are. Similarly, outsourcing work to customers in the form self service is often not seen as problematic as it is assumed to be convenient and time saving for customers (as well as reducing costs for businesses). But self service assumes customers have access to the knowledge and technology needed to adequately serve themselves, when in fact segments of the population may be excluded and others not able to act in their own best interest. That labour is exploited to produce the materials needed to develop and deliver AI services is less obvious and largely obscured. In *Cobalt Red: How the blood of the Congo powers our lives*, Kara notes that "no company wants to concede that the rechargeable batteries used to power smartphones, tablets, laptops and electric vehicles contain cobalt mined by peasants and children in hazardous conditions" (2023, p.10).

Interactions with AI that are disconcerting or inconvenient erode trust and raise questions – these interactions may not necessarily harm individuals but may potentially harm a financial institution's reputation and revenue. These can include frustrating or inappropriate interactions with chat bots,

messaging (texts, email) perceived as intrusive or 'creepy", or incorrect account flags. For example, automated fraud detection that may at one point may flag non fraudulent activity (such as when you find your credit card use has been suspended and you must contact the bank because of an unusual but legitimate transaction) while at another time allow actual fraudulent transactions through (which must then be disputed with the bank) may result in limited harm (other than to those who mistakenly pay fraudulent charges) but raise doubts and concerns about the functioning of the bank.

Greater than harm to any one bank are threats to the stability of the whole financial industry. The 2008 global financial crisis and subsequent 'great recession' has been in part blamed on lax regulatory oversight of flawed risk models (Colander et al, 2009; Crotty, 2009; Truby et al, 2020). Today the adoption of complex and increasingly opaque AI driven models; the accelerating connection of disparate data sets; and growing presence of third-party suppliers, from fintech services for individuals through to the various AI software that the banks depend on, present new risks to financial stability. Cyber attacks, which affected 18% of business in Canada in 2021 (Statistics Canada, 2022), are one of these. Intentional and unintentional data leaks open people up to identity theft and financial loss. The international monetary fund notes that "most worrisome are incidents that corrupt the integrity of financial data, such as records, algorithms, and transactions" which "pose a growing threat to the global financial system, financial stability, and confidence in the integrity of the system" (Maurer & Nelson, n.d.) Even more alarming are unforeseen threats. As Truby et al note, "One of the lessons from the 2008 financial crisis was that hubris can be catastrophic" and

> "the risk of systemic instability is actually growing as economies are increasingly data-driven and that data is increasingly interconnected. The prospect of contagion is now a real

> risk with far-reaching disruptive potential given the extent to which data is wedded together across systems and sectors. As financial systems develop and continue to become intertwined across jurisdictions, instability or uncertainty infecting one area can quickly spread across the network. These ripples may be technical glitches arising from technological failures, but they are just as likely to be financial problems caused by improper practices or processes. (Truby et al, 2020, p.114)

The Bank of Canada identifies cyber security as a top vulnerability in the Canadian financial system, noting that "ultimately, public trust in the financial system rests on the ability of participants to protect the day-to-day functioning of the system." (Macklem et al., 2022).

The potential harms associated with AI and data practices are extensive. As part of the findings of this study, I will evaluate which harms are represented and how in the banks' framing and communication of data practices. This in turn will provide insight into implications for future policy and governance.

CHAPTER 3: METHODS AND METHODOLOGY

In order to develop a comprehensive perspective on the transparency practices related to the governance and communication of the use of AI in the Canadian banking industry, I have employed a case study approach in two parts: an analysis of documents that communicate required disclosures, and a series of interviews with Canada's five biggest banks. While the methods and findings for each part are discussed separately, they are both designed to address the same over arching research questions and lead to implications for future policy and regulations.

The case study method is particularly suited to addressing the how and why of contemporary phenomena (Yin, 2018 p. 33) and a mixed method approach enables the researcher to "address more complicated research questions and collect a richer and stronger array of evidence than can be collected by any single method alone (ibid, p.100). Employing a combination of sources, methods and theoretical perspectives – documents and interviews, qualitative and quantitative methods, verifiable and performative perspectives on transparency - enables an in depth understanding of the current state of the banks' transparency practices as they relate to communicating their use of algorithms and automated decisioning. The comparison between the banks affords the development of generalizations around how transparency is used to both reveal and obscure data activities and implications for policy going forward. Importantly, both the interviews themselves and the process of securing the interviews are informative in this regard. Note that this study will not show how the banks' communications are received by the public or the press, nor enable us to know to what if any degree these communications allay concerns about the use of AI.

Findings from the document analysis and interviews will be first analyzed separately and then combined to address my research questions.

R1. How are data practices framed and communicated?

The findings for this question are addressed in the context of transparency practices: what is disclosed, how and for what purpose?

R2. What beliefs and values are expressed?

The findings for this question also include an evaluation of the harms addressed in comparison to the comprehensive list developed in the literature review.

Documents Methods

The banks publish a wide variety of documents on their websites that offer a public view into their business activities. These fall broadly into two categories: disclosures that are required by regulation or policy (either industry or governmental), including codes of conduct, corporate social responsibility reports, documents on various aspects of governance, privacy policies, and annual reports; and promotional material such as press releases, analyses, podcasts, and white papers. This thesis is confined to the first category as these disclosures, which, while not devoid of promotion are not strictly so, and can best provide insight into discourse around AI and how that intersects with policy. In order to uncover the extent and location of any mention of AI, each bank's website was searched using the site's own search function and these key words: AI, artificial intelligence, machine learning, and data.

Only privacy policies and annual reports are consistent sources across all five banks that address either AI or data or both and thus comprise the focus of documents analyzed in this study. There

is no mention of these terms in any corporate social responsibility related documents. Codes of conduct do make mention of data, but only in regard to employees' obligation to safeguard confidential bank and customer information and so are not included in this study.

Privacy policies are a long-standing corporate transparency practice: as Bruening and Culan note, "Since the late 1970s, what has commonly been referred to as notice has served to practically establish openness in most commercial transactions. Notice has been relied upon to inform individuals' decisions about the collection, processing, sharing, and reuse of their personal information." (2016. p.517). In Canada privacy policy requirements are governed by PIPEDA. While there is no current legislation requiring disclosure specifically about AI, PIPDA's guidance on consent states "organizations are generally required to obtain meaningful consent for the collection, use and disclosure of personal information" (Office of the Privacy Commissioner of Canada, 2021) and increasingly that use is to feed machine learning. The privacy policies of all the banks are available online, with links found in the small print at the bottom of each bank's webpages. Each bank has between two and six policies addressing privacy. All policies were downloaded or copied and pasted into Microsoft Word between March 26 and 27, 2021 and given the word count of each document was under 2500 words, the text search function was used to source the content relevant to AI practices.

Annual reports are a primary artifact of transparency for corporations, containing a combination of information required by regulation and industry norms to be disclosed along with information the banks choose to make public. The purpose of annual reports is to provide stakeholders (investors, regulators, employees, and customers) information they can use to determine the current financial stability and potential future growth of the bank. This analysis of annual reports looks at them not just as a professional practice but as a social practice within the framework of

ethnographic discourse analysis (Gee et all, 2012) and perspectives on transparency: how do annual reports shape our knowledge of and beliefs about AI – what reality is created by these disclosures?

The corpus linguistics method is used within this framework with the understanding that:

> "one of the key strengths of a CL approach is that quantitative and qualitative types of evidence can be joined up. Typically, the researcher will move back and forth between examining the frequencies of individual words and lexical bundles (also referred to as chunks, clusters, or n- grams) and searching for patterns of meaning in concordances. Combining the two perspectives can help in identifying salient themes and viewpoints expressed in the corpus. Thus, ultimately, lexical choices at the micro level can be related to macro- level textual phenomena … and social phenomena." (Friginal et al, 2021, p.321).

Given the reports averaged over 165,000 words, they were analyzed as a corpus using Voyant tools, an open-source web base text analysis environment. Each of the five 2021 Annual reports were downloaded July 18th, 2022. An iterative approach was taken: first searching for the terms 'AI' and 'artificial intelligence' to gather related terms based on proximity, and then searching for those related terms to understand context and evaluate whether or not they should be included in how AI is being defined by or used in the reports. In this way a short list of terms which could be determined to be pertinent to the discourse surrounding AI was established. This list of terms was then analyzed in terms of context in order uncover key themes appearing across the documents. Each theme identified was further examined to evaluate what was being disclosed or obscured and what values and believes were expressed or implied.

In addition, readability is evaluated as a qualitative measure of the potential purpose and effectiveness of both the privacy policies and annual reports: how do these disclosures function as a transparency practice? Automated decisioning practices are complex and the readability of disclosures is indicative of who might understand what is being communicated (such as the general public or experts) and what purpose is served (such as a purported disclosure that in fact obscures due to lack of intelligibility). Readability is measured using the Microsoft Word documents stats function which provides Flesch Reading Ease and Flesh-Kincaid Reading Grade Level scores. Flesch-Kincaid is a well validated method that has been applied in other studies evaluating the readability of privacy policies (Das et al, 2018; Fowler et al 2020; Li et al 2012; Zang et al 2020). The Flesch Reading Ease test evaluates the length of sentences and words to calculate a readability score ranging from 0 to 100. The higher the score the easier the text is to read. The Flesh-Kincaid Reading Grade Level test calculates the mean sentence and word length to arrive a score ranging from 1 to 18, corresponding to US school grade levels. Scores higher than 12 correspond with college or university education.

The document analysis portion of this case study includes both regulated and unregulated discourse and will be largely quantitative. Examining transparency practices that are required by regulation and those that are selected by the banks will answer what is disclosed, how and for what purpose and provide insight into the banks' beliefs and values.

Interview Methods

The interview portion of this case study provides a qualitative approach to the research questions. It offers the opportunity to probe more deeply on the practices of the banks to better understand how the communication of the use of AI is approached and what beliefs and values are expressed.

Interviews were drawn from the five largest banks in Canada: TD, RBC, Scotiabank, BMO, and CIBC). As mentioned, altogether these five banks account for 85% of the banking market in Canada, effectively establishing an oligarchy and providing an ideal focus of analysis. Interviewees were sourced via referrals through existing professional contacts and by connecting with media relation contacts named on the banks' websites between October 2022 and January 2023 with a goal of two interviews at each of the five banks. Ideal potential interviewees were identified as being senior executives in the areas of corporate communications, innovation and automation, and/or data and technology willing and able to speak about the bank's AI activities and how they are communicated to the public. In total 7 interviews ranging between 30 and 60 minutes were secured across all five banks and conducted between January 13 and March 1, 2023. In each case, contacts directed me to leaders in data and analytics as being best able to address my questions.

Interviews were semi structured with broad open-ended questions that would allow interviewees to speak to their areas of expertise and to not only gather answers but to also provide insight into what information would be shared and how - I viewed the interviews themselves as a transparency practice: what would the banks disclose and to what purpose? The questions asked were also designed to provide insight into what harms the banks are addressing and how. In this way each question contributes to answering one or both of my research questions (how data practices are framed and communicated and what beliefs and values are expressed) as well allowing for additional findings so that implications for future policy and governance could be developed.

The questions were as follows, with the expected types of findings noted:

1. Can you describe the ways in which the bank uses automated decision making/AI as part of products and services offered to customers? How does the bank communicate to customers about the use of automated decision making?

   Expected Findings: How are data practices are framed and communicated? What will be disclosed to me? What is being disclosed to the public?

2. What are the advantages or benefits of using automated decision/AI making as part of these products or services for the bank? For consumers? Can you share any specific examples of where the bank has realized this advantage? Where the consumer has?

   Expected Findings: How are data practices are framed and communicated? What values and beliefs are expressed?

3. Some academics and journalists have raised concerns about the use of automated decision making/AI. Are you and your colleagues aware of these concerns? What if any specific concerns are you aware of? What activities has the bank undertaken to address these concerns?

   Expected Findings: What values and beliefs are expressed? What harms are the banks addressing? What governance practices are in place that may have implications for policy and/or effectively addressing harms?

4. There have been calls for greater transparency about the use of data and automated decision making. Bill C-27's Artificial Intelligence and Data Act requires that "a person who manages the operation of a high-impact (artificial intelligence) system must, in the time and

manner that may be prescribed by regulation, publish on a publicly available website a plain-language description of the system that includes an explanation of how the system is used; the types of content that it generates and the decisions, recommendations or predictions that it makes". What challenges does the bank face in addressing this requirement?

Expected Findings: What values and beliefs are expressed? What will be disclosed to me? What is being disclosed to the public? What might future disclosures look like?

It is important to note that even though all five banks were asked the same set of questions it cannot be assumed that any one answer does or does not apply to any other or all of the banks. Responses were informed by the interviewees' particular area of expertise, what they thought was important or top of mind, their understanding of the question, and what they were willing to share. Responses cannot be seen as providing a comprehensive view of industry practices but rather are suggestive of the state of these practices.

Chapter 4: Findings

This section reviews the findings based on each of the methods detailed, starting with the documents followed by the interviews. The section concludes with a discussion of how the findings, considered as a whole and evaluated as a set of transparency practices, answer the research questions.

Documents

Readability

An evaluation of the readability of the documents reveals that they function more as performative than verifiable transparency (Albu & Flyverbom, 2019): the language level obscures more than informs. While PIPEDA does not stipulate a reading level for Canadian privacy policies, the government of Canada does recommend a reading level of grade 6 to 8 for Informed Consent Documents for science and health research participation (Canada, 2004) and a reading level of grade 7 to 9 for correspondence to citizens issued by the Social Security Tribunal of Canada (Tribunal, 2019). Importantly, the government initiative to modernize PIPEDA via Bill C-27 which includes both the Personal Information and Data Protection Tribunal Act and the Artificial intelligence and Data Act, include requirements for "plain language" disclosures to the public regarding both use of data and of AI (Parliament of Canada, n.d.). The average Flesh-Kincaid Reading Grade Level for the privacy policies of Canada's five big banks is 14.1, requiring a post-secondary reading ability, well above the maximum grade nine level recommended by the government for other types of documents that are required to be understood by the public. The average reading ease score is 35.1, which is rated as difficult to read (Flesch, 1949, pp.150). Similarly, the five annual reports require a well-educated reader, with an average Flesch Reading

Ease score of 25.4 and a Flesh-Kincaid Reading Grade Level of 13.9. See chart below for the scores for each bank. As has been demonstrated in other analysis of privacy policies (Das et al, 2018; Fowler et al 2020; Li et al 2012; Obar, 2022; Zang et al 2020), the bank's policies do not meet a standard of transparency that requires understanding and therefore do little to empower consumer choice.

Table 1: Readability of policies and reports

Document	Per Microsoft Word Document Stats	BMO	CIBC	RBC	Scotiabank	TD	Average
Privacy policies	Flesch Kincaid Reading Ease	36.0	33.8	36.6	32.0	37.0	35.1
	Flesch Kincaid Grade Level	13.8	14.5	13.2	14.9	14.2	14.1
Annual Reports	Flesch Kincaid Reading Ease	24.9	25.4	24.6	25.0	27.2	25.4
	Flesch Kincaid Grade Level	13.7	14.1	14.6	13.6	13.3	13.9

Mention of AI and related practices

There is no explicit mention of automated decision making, algorithms and/or artificial intelligence in the privacy policies, not a surprise given this is not at this time required by law. All of the banks address interest or behavioral based advertising, discuss the use of cookies and tagging or tracking, and use either 'customization' or 'personalization' in the context of advertising. It is unlikely given the technical nature of the topic and reading level of the documents that the average reader would connect these practices with automated decision making. Three of the five banks refer to the making of predictions, with this statement from CIBC providing the most detail:

> "We may de-identify or anonymize your information by removing identifiable information such as your name, address, date of birth and account numbers. Such information may be aggregated with other information and used for internal business purposes such as analytics and reporting, developing and improving our products and services, understanding and

predicting client needs and preferences, preventing and detecting fraud, identifying trends like purchasing patterns, fraud trends, or enhancing our marketing."

All of the activities described above may involve the use of automated decision making or artificial intelligence. However, the information is insufficient for even an expert to know for certain to what degree these practices are employed.

The annual reports do make explicit references to AI; however, it is a minor subject, making 37 appearances (either as AI or artificial intelligence) over the five documents which contain 829,180 total words and 37,156 unique word forms. This is lower than two other key topics of social concern: the environment (the word environmental appears 193 times) and diversity and inclusion (the word diversity appears 59 times).

Representations of AI in the annual reports

The initial visual scan of the documents' layouts and design and preliminary investigation into AI and associated terms revealed that all five reports can clearly be divided into two very different sections. The first section focuses on selling the banks' strengths and successes through a combination of graphics, charts, photographs, and statements. This section includes highlights for the year and messages from the Chair of the Board of Directors and from the CEO. All reports make extensive use of colour and design in this first section with font sizes ranging from 8 to 21 points (excluding titles). The second part, entitled Management's Discussion and Analysis (MD&A), provides the information required by the Enhanced Disclosure Task Force (EDTF) which was established by the Financial Stability Board in 2012 to identify fundamental disclosure principles, recommendations, and leading practices to enhance risk disclosures of banks. This section features primarily text and tables with font size ranging from 6 to 8 points (excluding titles).

The layout of the reports in this manner clearly differentiates what the banks want to disclose (part one) and what the bank must disclose (part two). Subsequent analysis focuses on each of these sections separately.

Section one (Highlights, CEO and Chairman letters)

The upfront section of the annual reports focuses on information the banks chose to report, functioning as performative transparency or "visibility management' (Flyverbom, 2015; Stohl et.al, 2016). As Lightstone and Driscoll note in their analysis of press releases from companies trading on the Toronto Stock Exchange, unlike the publication of formal financial statements (such as the ones included in an MD&A) there is no regulation or oversight of the public disclosure of qualitative information by corporations (Lightstone & Driscoll, 2008). AI and related terms are not predominant in this section (the words 'AI' or 'artificial intelligence' appear only 12 times out of 3,854 unique word forms across the first section of the five reports), dwarfed by highlights of financial results and attention to environmental and diversity and inclusion initiatives.

The language around AI in the reports is best characterized as vague and positive. We see the term joined with others like "data", "personalized", "analytics" and digital" which hint at the work of algorithms on big data sets and the outcomes experienced online and in mobile apps. In the case of CIBC, they simply mention "digital enhancements" and "data-driven decisions". This language obscures the vast assemblage that makes up AI. Instead, AI is made to appear as a mysterious force with the 'power' to deliver better customer experiences as seen in these sample statements taken from each report:

> "We are harnessing data and artificial intelligence to deliver even more personalized experiences. By leveraging analytics, we can deliver a more seamlessly integrated value proposition to our customers" (BMO)
>
> "Our investment in market-leading public cloud technology will reinforce and expand critical foundations in data protection and security and enable us to support faster, real-time, data-driven decisions, to quickly launch and scale new innovations for enhanced client experience." (CIBC)
>
> "As a leader in harnessing the power of artificial intelligence (AI) solutions, for years we've been empowering clients, simplifying and digitizing their interactions with us – saving them time, adding convenience and delivering meaningful value and insights which has fostered stronger relationships." (RBC)
>
> "…we introduced ScotiaRED—a series of state-of-the-art electronic trading tools that deliver high-quality execution using advanced analytics and artificial intelligence…enhancing performance and providing a superior client experience across" (Scotiabank)
>
> …continued to integrate AI to offer customers more personalized, connected digital experiences" (TD)

The discourse around AI supports the Annual Report's function of demonstrating each bank's current and future potential financial health by emphasizing leadership in 'harnessing', 'leveraging', 'introducing' and "integrating" technology advancements: stakeholders should feel confident that the banks are at forefront of realizing the 'power' of AI. The experiences the banks offer customers are 'personalized', 'connected', "convenient", and 'simplified'. Nowhere is the

'power' of AI or related activities directly associated with specific revenue opportunities like cost savings due to automation, increased customer retention, or growing market share. Only the BMO statement, "we can deliver a more seamlessly integrated value proposition to our customers" provides a bare hint of the possibility of increasing the sale of additional products and services through AI. Instead, the discourse relies on implicit assumptions that the reader may make: that AI improves the customer's experience with the bank, that customers desire increased personalization, and that such experiences will lead to better financial outcomes for the banks.

Section 2 MD&A

The MD&A section of each bank's annual report is governed by disclosure principles developed by the Financial Stability Board and the International Financial Reporting Standards Foundation (IFRS) and required by Canadian Law under section 4.6 of National Instrument 51-102 - Continuous Disclosure Obligations (Ontario Securities Commission. (n.d.). Per their mission statement, "IFRS Standards bring transparency by enhancing the international comparability and quality of financial information, enabling investors and other market participants to make informed economic decisions." (IFRS, n.d.). The MD&A section clearly exists in the context of the belief in the power of transparency to defeat corruption, ensure accountability and create trust as encapsulated Brandeis' oft used quote "Sunlight is said to be the best of disinfectants; electric light the most efficient policeman". (Brandeis, 1913). This belief, along with the attendant belief in the rational actor and the idea that 'if I have factual information, I will make better decisions' (Hong, 2020, p. 38; Etzioni, 2019, p. 190; Flyverbom, 2019, p.13), has informed corporate disclosure practices and regulation for almost 100 years.

While MD&A section provides detailed financial results, the primary discourse within this section is one of risk management and mitigation (the word 'risk' is the most common word in this

section appearing 6608 times with ‘finance’ a distant second at 4888 times). There are two themes in the risk discourse: details about the actions the banks take to manage risk and caveats about limits of risk mitigation. Both of these themes intersect with the concept of AI.

In addition to mentions of “AI” and “artificial intelligence”, the terms “machine learning” and “algorithm” appear in the second section of some of the reports. Importantly these terms appear in conjunction with terms “model” and “modeling” in three of the five reports. What emerges is a subject defined as inclusive of a cluster of practices within the bank that require risk management. For example, BMO asserts “Model risk arises from the use of quantitative analytical tools that apply statistical, mathematical, economic, algorithmic or other advanced techniques, such as artificial intelligence (AI) and machine learning (ML), to process input data and generate quantitative estimates”, RBC states “We continue to evolve our governance model to take into account any new risk considerations that may emerge from the growing use of Artificial Intelligence (AI) methods and applications in our models”, while TD notes “The adoption of certain technologies, such as cloud computing, artificial intelligence, machine learning, robotics, and process automation call for continued focus and investment to manage the Bank’s risks effectively”. AI is situated as part of a group of ‘techniques” employed by the banks that represent a variety of risks including cyber attacks, data breaches and leaks, misuse of personal data, and misused or incorrect model results. As CIBC notes. “Resulting implications from failing to manage data and privacy risks could include financial loss, theft of intellectual property and/or confidential information, litigation, enhanced regulatory attention and penalties, as well as reputational damage.”

All five banks outline what they have in place to address these risks, with approaches clearly driven by regulatory requirements. All the banks have people and processes in place to manage

data privacy compliance, such as Privacy Officers and data risk management policies, in keeping with the regulatory requirements and related guidances associated with PIPEDA. They also have people and processes in place to address model risk management as stipulated by a guideline published by the Office of the Superintendent of Financial Institutions (Office of the Superintendent of Financial Institutions, 2021). These practices are outlined in detail in the reports.

AI is also mentioned in conjunction with caveats regarding risk mitigation and the limits of the bank to meet every possibility. CIBC notes that outside forces may create issues that the bank cannot control: "Our potential exposure to these risks increases as we continue to partner with third-party service providers and adopting new business models and technologies (e.g., cloud computing, AI and machine learning). Attackers gravitate towards vulnerabilities in an ecosystem, and the weakest link in the supply chain can be a supplier or third-party service provider, who may not have sufficiently robust controls". CIBC also calls attention to the possibility of new risks that the bank will need to adapt to: "while the adoption of new technologies, such as AI and machine learning, presents opportunities for us, it could result in new and complex strategic, reputational, operational, regulatory and compliance risks that would need to be managed effectively."

In addition to the discourse of risk, AI is mentioned as part of the more detailed review of accomplishments and goals highlighted in the first section of the reports. Here again the language largely defaults to undefined concepts and practices associated with positive sentiments:

CIBC notes "Advances in artificial intelligence (AI) and automation also have the potential to transform business models over time, including the delivery of financial services advice through automated processes."

BMO will "Deploy digital-first capabilities with an increased focus on data, analytics and artificial intelligence to drive simplification and scale."

TD "is advancing its artificial intelligence (AI) capabilities, to help further inform the Bank's business decisions and risk management practices as well as improve customer experiences and efficiency of business operations."

The discourse here extends beyond the power of AI to deliver a better customer experience that was the focus of the first section. AI is positioned as a capability of the bank to address risk management and business decisions and drive automation and scale. CIBC is the only bank to acknowledge the role of fairness and ethics in maintaining consumer confidence and trust: "CIBC is maturing its AI capabilities with a focus on maintaining customer confidence and trust by building AI practices that apply principles such as fairness, ethics, transparency and security."

Although the purpose of the MD&A section is to provide more details about the financial health of the banks, given the lack of regulation regarding disclosing AI related practices, it is not surprising that are only a few instances where AI is discussed in more specific terms:

"Aiden® is an AI-based electronic trading platform that uses the computational power of deep reinforcement learning in its pursuit of improved trading results and insights for clients." (RBC footnote)

"Launched BMO CashTrackTM Insights, an artificial intelligence-driven capability that to date has offered more than 180,000 insights to customers through our mobile banking app, helping them avoid cash shortfalls or overdraft fees and make real financial progress" (BMO)

"Launched C.MEE, an AI-driven technology that leverages data to enable more positive customer experiences, by analyzing data across customer touchpoints to provide the most relevant advice for our customers." (Scotiabank)

In these instances, AI is imbued with agency "in its pursuit…of results", "helping" and "provid(ing)…advice".

Two clear discourses about AI emerge across the five documents and two sections: one informed by regulation and what must be disclosed, the discourse of risk; and the other centered on what the banks want to disclose, the discourse of the power of AI. Across both discourses the discussion of AI lacks specificity, which along with the difficulty in reading level, serves to increase "the burden of following ideas in the text, which is a strategy of the management staff" (Qian,2020, p.428). The reader is not expected to understand or challenge what is presented.

The discourse of risk focuses on the risks to the financial health of the bank with risk to individuals positioned not as harm to people but as potential threats to the trust in and the reputation of the banks. With only a single mention of ethics in relation to AI, the banks assiduously avoid raising any of the concerns voiced by academics and journalists about AI and big data. Instead, extensive note is made of the people and processes in place, as required by regulation, to mitigate risk. We are not clear exactly what these people and processes are doing but should be assured that they are in place to manage any issues that may arise.

This analysis demonstrates managed visibilities (Flyverbom, 2016; Stohl et.al, 2016) at work. The benefits of AI are featured while specific data uses and practices are obscured. As other studies have shown, privacy policies, difficult to find and difficult to understand, are designed to maximize the amount of data collected and uses to which it can be put. Annual reports are designed to

reassure stakeholders that the banks are well managed with bright futures, with specific details limited to what is required regulation. Disclosures follow the letter of the law, not the spirit.

Interviews

Although I made clear that to each person I contacted at each bank that I was interested in learning about how the data practices and the use of AI were communicated to the public, I left it up to those I contacted to recommend the appropriate people to speak to. For four of the five banks, the interviews were arranged though the media contact person that usually deals with the press. In each case I was directed to an enterprise level leader in data and analytics. The titles of the interviewees included VP Advanced Analytics and Artificial Intelligence, Managing Director Data Science and Artificial Intelligence, AVP Data and Analytics, Senior Director Enterprise Data Management, Senior Director Data Advisory, and Senior Manager Data Ethics. All of the contacts made through my own professional network felt unqualified to speak about AI. The one that did agree to speak to me, a VP of Marketing, took care to warn me that they may not be able to answer most of my questions as they did not work in the "AI field" although in fact we were able to have a robust discussion around all four questions. This person subsequently referred me to a data and analytics executive at their bank. This suggests that data and AI practices are seen as highly specialized, perhaps even intimidating to most, requiring technical experts to address, this despite the myriad of people involved in the development, management, and use of AI systems. Given that most of the interviews were secured through official channels (the media/press contact), it can be assumed that interviewees are speaking on behalf of the banks.

In order to protect their anonymity, interviewees are referred to by numbers 1 through 7. Numbers were randomly assigned. After each quote used, the number assigned to that interviewee is noted in brackets.

While interviewees were generally willing to speak openly, not all answers were complete. None of the banks were completely open about all the ways in which AI is being deployed. It must be noted that it cannot be determined the degree to which this is due to being cautious about what was disclosed: "without giving away anything proprietary…" (6), versus not being able to disclose due to the particular area of specialization of the interviewee: "one thing that I might not be too helpful in this conversation is the product side, because we actually have a product analytics team within the bank, and even though I am the enterprise advanced analytics and AI lead, that's one area, that I don't do, and my team doesn't do, because we have a specialized team on the product side, we have a specialized team on risk and we also have a specialized team in info security fusion and capital markets" (2). In either case, we cannot assume that any one answer does or does not apply to any other or all the banks. In both cases, we see barriers to fully transparent communication.

Taken as a whole, four themes emerged from these interviews: communicating to the public about AI is an underdeveloped practice, the banks are keen to demonstrate governance, the view of potential risks and harms is narrow, and the banks struggle to balance caution with the need to compete.

Communicating about AI

Despite making it clear to communication professionals that I am a communications student interested in communication practices, I was consistently directed to data science experts to interview, each of whom worked in different divisions or departments of the banks. While all of these people spoke knowledgeably to most of my questions, they could say little about communicating with the public. This indicates that the banks have not developed a practice or assigned experts for communicating to the public about AI. As one interviewee put it:

> "To my knowledge there is no direct communication sort of you know, giving disclaimers ahead of time, but we are very open about the type of projects that we are working on, and a lot of these examples that I've talked about you can find articles about, and there's a lot of talk about that so it is made our customers are made aware that way. But right now, it is something that is being looked into, with, as you said, the new regulations coming in. I was just at a call yesterday where there were discussions around giving specific disclaimers around automated decision making to customers, so that's in the works, but to my knowledge, is not currently implemented at that level." (7)

The majority of communication from the banks about AI is unregulated: promotional communication in press releases, blog posts and advertisements. Regulated communication at present is limited to what we saw in the privacy policies and annual reports.

Several interviewees pointed out challenges with Bill C-27's proposed requirement to provide plain language disclosure about the use of AI. A key concern is the level of complexity and uncertainty about being able to disclose in a meaningful way: "we have hundreds of use cases, and they have their own nuances, and they have their own objectives and outcomes so to generalize it's impossible" (4). Achieving plain language is seen as potentially problematic: "any regulatory type of notification can be quite challenging to put into plain language because there's also legal

departments that are very involved and who can change a lot of the language to be sure from a legal standpoint its describing things in a proper way" (5). One interviewee echoed Stahl et al.'s finding in their paper "Organisational responses to the ethical issues of artificial intelligence" (2021) that companies wrestle with what constitutes appropriate detail: "you have to balance the details you publish because number one it's proprietary and number two as soon as you release details about that kind of stuff, it's easier for the less ethical people out there to game it" (6).

These concerns call into question whether disclosures about AI use can function as transparency in terms of empowering the public to make informed choices. It is more likely we will see transparency enacted as end in itself, fulfilling regulatory requirements but doing nothing to address the power imbalance between those collecting data and those providing it – as has been shown to be the case in data privacy disclosures. Here an interviewee reflects on what is being done in the EU, noting that AI details should be made transparent while at the same acknowledging they will likely be ignored:

> "I what I've seen that I really enjoyed is when you get a high-level summary so you know we will use your data for automated decision making and then maybe a couple of high-level bullets of what this is about, but then the option to click and read the details if you want. So, I don't think that we should take that option away from people. I think it's very important that all the details are there for the sake of transparency. But also recognizing that people don't always have the capacity, the time, the interests to go into that level of detail, so make it easy for them but still keep the information there in case it needs to be accessed." (7)

Interviewees also raised concerns about disclosure and consent requirements that may be confusing or onerous for individuals reducing the number of people agreeing to the use of their

data and the employment of AI: "…then people default to no to everything and then we lose valuable data that again could be used for certain purposes that the customer may have actually liked" (7).

Everyone interviewed supported the idea of transparency: "We have to be transparent, and I think most practitioners will probably tell you that it's good practice to be to have transparency as well" (4). But while transparency was seen as an unquestioned good in concept, in practice interviewees wrestled with how disclosures about AI and practices could or should be made. One interviewee hoped that the requirements for up front disclosures would not materialize, and legislation would focus only on explainability on request: "We'll see how the legislation shapes up and comes out eventually but I'm really hoping it will be more on an individual basis. Should we be communicating the results if someone comes and asks us, hey why? Why did you make this decision on my file? Yes, I think we should absolutely be able to explain that." (2)

Interviewees were mindful of the need to be able to explain AI decision making both internally and to customers who may question decisions about them. One person mentioned that 'explainability frameworks' are in use at their bank, but again, this does not necessarily mean that these are not in use at the other banks, only not mentioned. Avoiding the application of AI that is difficult to explain appears to be a key tactics for most if not all the banks:

> "a lot of times we use black box models, and we don't want do that where an explanation is needed for our customers, or even internally, in terms of how certain decisions have been made" (7)

> "if you're going to use something that it's very difficult to diagnose and explainability is a requirement then you default back to something that might be a little less complicated"(6)

Given that public disclosures are not at present mandated by legislation, it is not surprising the banks have given this area limited consideration. As mentioned, this is not to say that there is no communication to the public about AI outside the annual reports –promotional materials talk to the banks' investments in AI and the benefits it brings to customers - but an evaluation of these types of documents is outside the scope of this study. In terms of transparency practices at this point in time, the banks are much more inwardly focused on governance than outwardly focused on keeping the public informed.

Demonstrating Governance

Much of current regulation focuses on governance. For example, PIPEDA requires companies to have a Privacy Officer and the OFSI requires banks to have a board risk committee and Chief Risk Officer. As we saw in the annual reports, communicating about AI is more about communicating about how AI is governed than how or why AI is applied. Interviewees at all five banks were eager to let me know about practices they had in place to manage AI and ensure negative outcomes are avoided. This is an area that the banks are accustomed to being transparent about and all the people I was directed to speak with were knowledgeable about governance. Most of the AI governance practices are extensions of practices already in place to manage privacy, data, and models. These are the most developed practices:

> "… so this is managed by privacy and security and all data groups will have to have an agreement put in place that stipulates what you can and cannot use data for and how what data can you have access to, and what you can do, and how you can use it, and how you should not use it. So, it's a very detailed process that the team goes through, especially when it's a new team that has started up. They go through that whole process, and it takes

months, and once privacy is convinced that now you now understand what you can and cannot do, it's written, documented, and approved. Then you go." (4)

"We are rolling out a strong data governance framework which is trying to establish ownership and stewardship around data. So if we look at all data at (the bank), its client data, etc., how do we ensure that there are very specific rules that are looking at all aspects of data governance all the way from definition, to its data quality, to where it's source from, to the fit for purpose for usage, etc. and we're trying to create transparency around catalogs, what's in our systems, etc. So that foundational data governance becomes almost a prerequisite for when somebody wants to build a model. To make sure that the data foundation layer there's appropriate accountability from a people perspective, there's appropriate processes in place to make sure and procedures to make sure that the data is cataloged, understood, transparent, of quality within the system, and then it's supported by tools, so that almost becomes a basic, very basic, foundational step one to driving transparency." (3)

In some cases, the banks are building new teams and processes. One of the banks has had a dedicated data ethics team in place for about two years which they believe to be "one of the first in the North American and definitely in the Canadian space to do this." (7) Other banks spoke to having a data ethics committee or data review board that includes leaders across various functions including privacy and data governance. Several interviewees talked about the need to ensure staff are thinking not just about compliance to regulation but also the fact that "just because you can do something doesn't mean you should" (7). The focus of these practices is characterized as data ethics not AI ethics, suggesting that the banks believe that ethical issues are rooted in the data side of the AI equation, not the algorithmic. One interviewee explained that "these kinds of issues go

beyond just the use of data with AI and ML, but issues can happen throughout the whole data life cycle from the point of data collection to its management, sharing, and use with other methodologies as well, so that's why we've taken a broader data ethics approach at the bank" (7). At present these practices center around awareness and education, with lots of cross functional meetings and discussion:

> " We do have a Data Ethics Council that meets on a weekly basis and it has all of the key partners within our bank like, say, risk, legal, privacy, operations, me, my team and the business partners come in for every use case that they built, and then we have to discuss these things …So people actually come to the Council, we ask the questions, so they start hearing those questions, and once they start hearing those questions, our hope is next time they go and build something, they're already thinking about those questions because they know the recommendations on those questions. Right? So, it's part of the awareness and communications... It's the Council where we have to start to have that communication and awareness at the executive level" (2)

> "We have a tool called the Ethics Assistant… it's basically something that our AI and machine learning models that are being developed need to go through right now… We have 6 different ethics related dimensions, and the tool basically asks the questions and then based on the answer, it gives them a sort of rating in terms of how much ethical consideration and action may be needed for that specific model… along with that, we are currently building a data ethics framework…And then we have some other processes around sensitive data making sure that it's properly classified, and that we have a good enterprise level understanding of the sensitivity level of our data so that we can take the appropriate steps to you know ensure that they have appropriate access protection." (7)

> "Our communication mechanisms vary team by team…We have forums, we have ask me anything sessions that we put together to adopt that change, and that education for each of them, so that they're kept well informed about what is expected of them as the world evolves in this space…So a lot of it comes down to educating people, making sure that they fully understand these risks and why it's important for us to consider them. We have the principles, we do different kinds of live training, we have resources, and then we have our tools and processes." (1)

Interviewees were frank about AI governance being a work in progress:

> "So, we have been on a journey looking at a more, I guess, holistic AI governance approach in the last 12 months, and it's a journey. I don't think it's ever going to be completed, knowing the AI space is a constantly changing space, and the social concerns not just ethical, but social concerns are constantly gonna come our way. So we're on a journey. We started an AI governance program a year ago, and we're continuing to build on top of it. We have our trustworthy AI principles, and we're building all of those principles one by one, six principles. Two of them are already core to our bank, which is privacy and security, and the rest, four, we have been on a journey to build out - what does say accountability mean, transparency mean, like that is explainable to me? And how do we include that in our daily processes and tools and systems? How do we create more awareness and education so data scientists don't think that my job is only to build a model, but they know that their jobs are building responsible models. Right? So we're on a journey, again as I said, we're building the right tools and processes into our everyday model building approach, and we'll continue to do that. I think it's a never-ending evolution." (2)

> "I think it's an evolving conversation, right? The thinking is still pretty nascent on it. In our world it's very much a risk conversation, right, in terms of how we manage that. I do think the conversation is going to evolve into a bigger ethical angle, in terms of how AI is used, how it impacts people positively, negatively, if they even know about it…I think the thinking on impact and transparency and managing it is lagging the actual technical development of it and I think those two need to be in two swim lanes being pushed at the same speed" (6)

The view of potential risks and harms

That the banks have a narrow view of harm that is framed in the discourse of risk to the financial stability of the bank is as evident in the interviews as it was in the annual reports. The banks face various risks associated with AI as noted in the CIBC annual report including "financial loss, theft of intellectual property and/or confidential information, litigation, enhanced regulatory attention and penalties, as well as reputational damage". Everyone interviewed mentioned bias in response to my question regarding potential harms. Most spoke in some detail on the practices they have in place to ensure fairness including data hygiene and model testing work that has evolved over decades. Bias is problematic because regulations require that the banks be able to explain decisions (such as not approving a mortgage) when called upon to do so. A finding of bias represents a regulatory, litigious, and reputational risk. For this reason, managing bias is central to many data governance practices and the banks ensure their adjudication models are explainable.

The environmental impact of big data and AI was mentioned by one interviewee. They discussed including analytics as part of their environmental and social governance practice, which represents an opportunity to do good in a way that may enhance the bank's reputation and reduce costs:

> "One part of ethical data use, we thought, is also looking at its environmental impact. So now we are collaborating with that director and some academics to see if we can find a way of creating a framework for measuring and lowering the environmental impact of analytics…the footprint in terms of you know, all the resources that are being used in terms of electricity and all that". (7)

Other potential harms to individuals are not seen as problematic. AI that is employed to automate tasks, potentially creating job loss for individuals, is seen a benefit to the banks as it reduces costs, improves processing time, and removes the risk of "fat finger errors". One person talked about concerns raised by their team about potential loss of jobs which they dismissed saying "it shouldn't be a concern, because removing manual menial tasks and getting the machine to do it is a good thing, and the people who used to do that can be retrained and improve their skills to do other things". (4)

No one mentioned behavior modification or manipulation as a potential harm, despite it being called out as a concern by the FCAC. Propensity models were mentioned by two interviewees in response to the question about the banks' AI activities – models that predict, for example, your likelihood of purchasing a particular financial product. All the banks market offers to their customers and of course, they always have. The issue is, does technology make it too easy to say yes to offers that are more compellingly targeted than ever before? The banks are looking to make their offers more effective by ensuring they are as relevant as possible to you by presenting opportunities (for credit or investment) when you might need them most while at the same time balancing the risk of loss to the bank. Offers are designed to be in the banks' and shareholders' best interest first and in your interest only in so far as it does not impinge on those of the first two:

> "So we're looking to always find opportunities to drive revenue, right? So, if we're able to look at products and services, not at a granular level but just in general, banks make money on products like fees and interest, right? So, the advantages of being able to make decisions and do it in a timely manner - there's a revenue motivation to this. Also, it helps our clients with certain life events, right? So, when they need something, and they're in a time crunch, or we're in an economical turmoil like right now, and funds are needed, that's where we would want to target right?" (1)

It remains to be seen whether new or improved revenue streams enabled by AI will prove to be a win for both consumers and the banks. Typically, it is the consumer, not the bank, that has the most to lose. For example, online trading, increasingly automated and now marketed to young people, puts the risks on individuals not institutions: banks collect fees regardless of whether your investments grow or decline. The GameStop case covered in the literature review illustrates that the house always wins.

Balancing caution and the need to compete

Implementation of AI at the banks is about balancing caution – avoiding risk to revenue, reputation, and regulatory compliance – with the need to complete. AI investments that are low risk and contribute to the banks' competitiveness, such as those subject to little or no regulation that save time and money are already deployed by the banks. These include fraud detection, document management and chat bot applications. AI, aside from the most basic machine learning, is not applied where there is the greatest degree of oversight: risk models that are subject to audit or output decisions that may need to be explained. Here the banks appear to be defaulting to older tried and true methodologies where explainability will not be an issue. In this respect explainability

acts as a key restraint on the deployment of “deep learning” or “black box” AI. Several interviewees informed me that all models, including those not subject to regulatory scrutiny, are put through a rigorous multistage review process. But challenging the banks’ rigor and caution is the desire to be competitive by implementing more sophisticated AI. Interviewees noted that being competitive means providing the level of service customers want, and what they believe customers want is the same speed and convenience they experience elsewhere:

> “In general, I think it is becoming more and more of an expectation to have those kind of seamless experiences. I find myself even sometimes getting annoyed when Google doesn't automatically understand what I'm searching or what I'm trying to get to. So, I think there is a bit of that expectation” (7)

> “The expectations from the client is absolutely there. I remind all of our businesses, saying that hey we're not compared to RBC, we're not compared to TD, when you think about personalization. Because now I have the bank app on my phone and the most used app on my phone is most likely Amazon, so as a user, I compare my experience on every app to Amazon because they give me a beautiful user experience, right? Everything is personalized. Sometimes I see things and I'm like, yeah, that's actually what I was looking for, how did you know?...users expect it, clients just expect it… it’s just the normal expectation now.” (2)

> “it's a benefit for the bank and a benefit for the customer as well, because, you know, if the customer doesn't have to leave their house to actually deposit a cheque, right, they can do it in the comfort of their home, with their with their mobile device. It's super easy now” (5)

Delivering customer satisfaction is good for business: “there's an advantage to us from a better customer experience, there's an advantage to consumers from a better customer experience and it benefits, you know, shareholders and employees also.” (3).

Discussion

Looking at the research findings as a whole, clear and consistent patterns of discourse emerge that answer my research questions:

R1. How are data practices framed and communicated?

R2. What beliefs and values are expressed?

How are AI and data practices framed and communicated?

The research reveals that data and AI practices are predominantly framed in one of two ways: within the discourse of risk and within the discourse of customer service. While these discourses are communicated in a variety of formats and places, they are at all times informed by either regulation: what is required to be disclosed; or promotion: what the banks want to be known.

The banks are business, and as such employ AI to drive revenue and profitability. However, in framing and communicating data practices that fundamental reality is given little attention. There is some discussion of employing AI to create efficiencies (i.e., save costs). The annual reports make vague references to AI’s ability to “transform business models”, “drive simplification and scale” and improve the “efficiency of business operations”. Several interviewees noted that AI is being employed to automate various back-office functions. Only one interviewee called out the truth that they “are always looking for opportunities to drive revenue”. AI and data practices are

not explicitly framed in the context of how they deliver to the bottom line. Instead, we see AI presented within two distinct frames: risk and customer satisfaction.

All of the banks frame AI and data practices in the context of risk: what is the risk to the stability and profitability of the banks and how is that risk mitigated? In this context of risks, harms to individuals can only be perceived in so far as they impact the banks: will a finding of bias open the bank to litigation resulting in legal and settlement costs? Or diminish its reputation, resulting in lost customers and reduced investor confidence? The discourse of risks associated with AI coming from outside the banks, such as those from cyber attacks or third-party vendors are positioned as harms to the bank not individuals despite the fact the individual harm may result. AI is also a tool to address and reduce risk though fraud detection and cybersecurity as noted in several reports and interviews. In this way AI is both embedded in and subject to governance practices designed to mitigate risk.

The banks' attention to known risks – particularly data security and compliance to established privacy regulation – puts the banks' focus on data, not AI. The banks have data ethics committees and councils suggesting that the banks believe that ethical issues are rooted in the data side of the AI equation, not the algorithmic. The banks are still in the process of rolling out data governance frameworks, while AI specific governance frameworks are nascent or non-existent. The banks do not appear to be equipped to effectively manage AI applications that fall outside the frame of risk – such as those using anonymized data or large language models.

The frame of risk isn't necessarily a bad thing – our country needs stable banks. The banks' attention to risk meant Canada was saved the worst of the 2008 global financial crisis. However, when AI is viewed within the frame of risk to the financial stability of the bank, a lot can get left out of the picture: potential harms to individuals and society can go unrecognized, as can potential

benefits. Revenue and profit cannot be the sole focus of our financial industry to the exclusion of all else – that's why we have the Financial Consumer Agency of Canada. The FCAC's mandate is to protect the rights and interests of consumers of financial products and services, supervise the compliance of federally regulated financial entities with consumer protection measures and educate Canadians on financial literacy. The banks also recognize that it is to their benefit to demonstrate they have the interests of customers at heart by framing AI and data practices as practices in delivering customer satisfaction.

AI practices are framed as delivering customer satisfaction by being 'easy', 'time saving', 'convenient", 'relevant' and 'personalized', providing 'enhanced' customer experience. The frame of customer satisfaction provides behaviour guardrails at the banks as data practices that might generate customer complaints will be avoided. But it also puts pressure on accelerating AI adoption when customer satisfaction is viewed as providing 'seamless' experiences similar to technology companies. Connected data is at the heart of delivering those experiences, which requires customers to consent to their data being collected, shared, and applied. This in turn provides an incentive for the banks to facilitate consent – to make it easy to say yes and hard to say no – as we see in the way privacy policies are made difficult to find and understand as this and other studies cited have demonstrated (Das et al, 2018; Fowler et al 2020; Li et al 2012; Obar, 2022; Zang et al 2020). Disclosures about data practices are already designed in ways that ensure the banks can continue to accrue and leverage personal data and given proposed legislation, there is no reason to imagine that disclosures about AI practices will be any different.

In the document analysis we see two distinct ways of communicating to the public about AI, one informed by regulation (what the banks are required to say, predominantly framed in the context of risk) and one informed by self promotion (what the banks want to say, predominately framed in

the context of customer satisfaction). Regulated communications are focused on required disclosures. Information about data use is made available, but not particularly accessible or understandable. Visibilities are managed through language difficulty, formatting, document length and font size. Annual report content is focused on governance, framed in discourse of risk and designed to assure investors the banks are well run and forestall any scrutiny of the data and AI activities the bank is undertaking.

In the case of the interviews, no disclosure was required – they were not obliged to answer all my questions - and all elected to emphasized governance while most limited discussion of specific activities. Interviewees raised concerns about increased transparency requirements around AI and data use: that bad actors might misuse information, that its is too complex to explain, that constraints around explainability will stifle innovation and the adoption of AI, that some information is proprietary and should not be shared. It is clear that the banks will communicate what is required and are keen to demonstrate regulatory compliance. However, it is also clear that regulated communication to the public is simply information sharing – done to the letter of the law, not for the purpose of creating understanding.

The analysis of the annual reports demonstrated that outside regulated disclosures, communication about AI is overwhelmingly positive and vague. As noted, interviewees provided limited examples and few specifics. Visibility into the AI activities of the banks is carefully managed to ensure positive reception by customers and investors and to protect competitiveness. Pending requirements to disclose AI practices in plain language are seen as problematic and the banks appear to have not yet prepared themselves for these types of disclosures. While I had hoped to uncover more about how the banks communicate to the public about AI, the bulk of that work is done in the press and in advertising, an analysis of which is outside the scope of this thesis.

What beliefs and values are expressed?

The banks believe that the increasing deployment of AI is inevitable and inevitably good. The research reveals that driving the deployment of and communication about AI are two powerful beliefs: a belief in the preeminent virtue of efficiency and a belief in transparency as an unquestioned good.

Although the banks are (ironically!) not explicit that AI helps them save or make money, many of these practices deliver against one of the highest values in our busy, financialized society: efficiency. AI automates repetitive tasks. It enables the bank to act faster and address opportunities and threats sooner. Offers for more credit can be presented to you just when you most need it. It's critical in the cybersecurity where bank AIs battle bad guy AIs in real time. AI is seen as reducing errors and saving time. Efficiency is synonymous with capital accrual and profit.

The pursuit of efficiency also circumscribes choice. Under the guise of being easy and convenient many initiatives driven by the pursuit of efficiency increase self service and reduce jobs. Opportunities to interact with a real person have been steadily declining and the pressures on individuals to be financially and technologically literate have increased. The banks believe that customers want and expect more seamless digital experiences, but's not clear that desire is to the exclusion of human interaction and support – particularly when it means individuals assume more labour and more risk in the process. It's not my preference to interact with a chat bot and my investment with a self serve investment platform is significantly underperforming my investment with a financial advisor. However, directing customers to digital interactions saves costs and allows the banks to accrue more data.

Focusing only on efficiency when aggregating data and applying AI obscures potential harms. Obtaining consent for and securing personal data is seen as sufficient while issues with aggregated and anonymized data are ignored. Increased linking of data across applications and businesses opens up opportunities for data to be deanonymized or leaked, compromising privacy and increasing the threat of fraud. Profiling and targeting people with tempting offers easily accepted when they are vulnerable is seen as good business. Local labour impacts are not viewed as problematic and labour exploitation abroad is made invisible. The burden on individuals - to self serve, to buy new technology and learn new applications, to be proactively protecting themselves in everchanging digital spaces, and to be responsible for decisions they may not be equipped to make – is not even a consideration.

The banks also believe that transparency is 'good practice". However, it's perceived as something to be delivered: making information available, not necessarily understood. When information is shared with experts, like the OSFI and FCAC, transparency is essential to overseeing the good governance of the banks. Information shared with the public, however, is strictly performative. Data use disclosures in the bank's privacy policies meet regulatory requirements but they are difficult to find and understand. The interviews and annual reports emphasize the practices in place to manage AI but not how and why AI might be employed. Interviewees expressed resistance to pending regulation requiring plain language disclosures of how AI is deployed. The belief in transparency as an unquestioned good is clear, the understanding of or commitment to what transparency requirements in regulation are supposed to achieve is not. The disclosures examined in this study do not facilitate meaningful consent to data use nor do anything to address power asymmetries between individuals and the banks.

CHAPTER 5: CONCLUSIONS

I wanted to understand how Canada's five big banks framed and communicated AI practices and the values and beliefs expressed in order to create a foundation from which I could consider the implications for policy and public trust. I selected the banks because they have obligations to both shareholders and the public, they are heavily invested in AI, and they are heavily regulated.

The immediate threat to public trust in the banks as a result of data practices is low. Governance and regulation reduce risks and the banks have made both cyber security and attention to data leaks and misuse a priority. Documents and public discourse that obscure specific activities and emphasize customer satisfaction work at maintaining positive sentiment. It is far more likely that economic upheaval will shake trust – mortgage defaults and foreclosures are expected to rise in the coming months in the wake of higher interest rates. People are focused on how their credit and investments are managed, not what the banks are doing with technology. However, the findings of this study do have clear policy and regulatory implications for the private sector even outside the financial industry.

Banking, like health care, is heavily regulated, manages sensitive personal information, and has a profound effect on life of every Canadian. Importantly, regulation in the finance industry has long focused on computation, with decades of evolving governance requirements for risk modeling. It's unlikely that there are many other industries framing their AI and data practices in the context of risk to the degree that the banking industry does. But all industries are beginning to deploy AI across their businesses. All industries are collecting data: through loyalty programs, at point of sale and ecommerce, in apps and more. Many companies are acquiring business that allow them to expand the data sets they can use to train AI: Google now owns Fitbit, Loblaws owns Shoppers

Drug Mart and PC Financial (and has recently launched Loblaws Media to monetize their data). The potential for harm, from bias and exacerbations of inequities to social engineering and behavior modification to privacy breaches and identity theft, exists across a vast array of business. What can Canadian business and regulators learn from the current practices at Canada's big five banks as revealed by this case study?

Implications for Policy and Governance

The findings in this study demonstrate the potential power of regulation and the problems inherent in our reliance on performative transparency practices. The research suggests four opportunities to more effectively address potential harms arising from the use of AI:

1. Reframe risk
2. Challenge transparency practices that rely on individuals
3. Mandate AI for good
4. Include AI practices in Corporate Social Responsibility

Regulation is the only thing protecting Canadians from potential harms that may result from the ever-increasing aggregation of data and deployment of AI. Throughout this study and in the literature, we see that companies are challenged to meet the letter of the law and do not meet the spirit of the law. The banks are focused on compliance and good governance, but their fiduciary duty extends only as far as required. While data and AI ethics may be important to individuals in the bank, as an institution ethics is viewed in the context of risk and liability – harming people is an issue only insofar as doing so harms the bank.

The research shows that the banks proceed with caution when there is oversight. Requirements that models be explainable act as a constraint on the use of black box or deep learning AI in risk models. Other models, such as propensity models, while subject to internal governance practices, need only to deliver to the banks' objective of increasing revenue and improving profitability. It is not clear how AI initiatives outside models, such as chatbots and task automation, are governed beyond the application of capitalist logics. This is unlikely to change as Bill C-27 requires explainability only for 'high impact" applications of AI. While 'high impact' remains to be defined, it is certain that many applications of AI will not be subject to explainability and many potential harms arising from applications deemed low risk will go unchecked. However, this study of the Canadian banking industry suggests that the following approaches may address a broader conception of harm: reframing risk, challenging transparency, mandating AI for good, and considering data practices in the context of corporate social responsibility.

Reframing risk

This study demonstrates how framing AI practices in the context of risk, which for the banks is risk to their financial stability, narrows the perception of harm and what is required to effectively manage AI. Canada's AI regulatory framework, like the EU, is also risk based and subject to the same pitfalls in attempting to define and regulate 'high impact" AI systems. As De Cooman notes "Despite the statistical nature of risk regulation, rationality and scientific evidence are not the only drivers of the level of risk acceptability. Cultural and psychological dimensions also play a role." (2022, p.62). This is the reason we see widely varying levels of regulation around the world and over time for things like alcohol consumption and smoking. One remedy that has been proposed is that a rights-based framework to AI regulation be adopted. Policy advocates such as AccessNow

"propose that the burden of proof be on the entity wanting to develop or deploy the AI system to demonstrate that it does not violate human rights via a mandatory human rights impact assessment (HRIA)." (Leufer & Hidvegi, 2022). Other contend that all AI development and deployment be subject to governance and transparency regulations (ECNL, 2021) as limiting regulation to only "high impact' systems will likely miss the harms our Artificial Intelligence and Data Act purport to protect us from: "physical or psychological harm to an individual; damage to an individual's property; or economic loss to an individual" (Parliament of Canada, n.d.).

The widespread deployment of large language models (LLM), such as CHATGPT, which occurred during the writing of this thesis, is a case in point. It is likely that many applications of this AI will not fall under a designation of "high impact" and therefore disclosure of their use will not be required under current proposed legislation. However, I would contend that people have a right to know they are communicating with or receiving communication from an AI in all cases given interactions with large language models will influence people's decision-making across many aspects of daily life.

Challenging Transparency

This study demonstrates that current transparency practices that rely on individuals to make informed decisions or police harms do not work to deliver the promise of Canada's Digital Charter: that "Canadians will have control over what data they are sharing, who is using their personal data and for what purposes" (Government of Canada, 2023). The stipulation of plain language may remedy this to some degree, but as we have seen there is plenty of motivation for companies to design the content and presentation of their notices to make it easy to say yes and hard to say no. Giving consent and exercising control is challenging when options are not clear, implications are not understood and doing so may prevent us from accessing services we may want or need. Current

data practices effectively render consent and control meaningless as our personal data is aggregated, anonymized, shared and applied in ways we cannot follow and which no single entity controls. While existing data transparency regulations do not meet stated aims, the public transparency proposed in the Artificial Intelligence and Data act appears to set out to be strictly performative. Innovation, Science and Economic Development Canada states "Transparency means providing the public with appropriate information about how high-impact AI systems are being used" (Innovation, Science and Economic Development Canada, 2023).

I characterize this requirement for simple disclosure as performative as it does not create the opportunity for individual control or empowerment, a situation exasperated by its narrow application to high impact systems. A broader application of requirement to be transparent, such as when an LLM is in use, would be a start – at least people would made aware of where a recommendation or information is coming from. However, in most cases, high impact or not, simple disclosure will not enable choice if a needed service cannot be accessed in any other way except under the data and AI use a company has stipulated.

However, we do see transparency functioning to protect Canadians with experts, like the FCAC and OSFI in place to review and validate information. Expert oversight could be implemented for AI development and deployment across all industries in a number of ways. Non profit organizations such the Responsible Artificial Intelligence Institute are increasing employed by companies and governments (including Canada) to provide regulatory compliance assessments and responsible AI certification among other services. Such organizations could be themselves regulated or incorporated into the government and their audits made mandatory. Similarly, reports like The Data Privacy Transparency of Canadian Internet Carriers Report (Obar, 2019) could be formalized with remedial action and fines attached to noncompliance. The proposed AI and Data

Commissioner could proactively audit some applications of AI. Rigorous processes like the banks have in place for model development could be used as the template for proposed internal AI development governance requirements.

We also see transparency functioning to protect Canadians in the form of explainability requirements. The need to be able to explain how a model or AI application reached a decision or output acts as a restraint, keeping AI understandable to human stakeholders, as is the case with the banks' adjudication models. While such a restraint maybe characterized as stifling innovation, requirements like explainability can also foster creativity in terms of solutioning within a set of acceptable parameters. A broader application of the requirement of explainability is one way to address the alarms raised by leading AI pioneers such as Yoshua Bengio and Geoffrey Hinton, who have publicly called for slowing down AI deployment and speeding up the implementation of regulation (Coulton, 2023; Goodyear, 2023).

AI for good

One of the principles of Canada's Digital Charter is data and digital for good. As noted previously, FCAC regulation has evolved to recognize and harness the power of nudging for the public's benefit: "As of June 30, 2022, banks will be required to send new electronic alerts to their customers. The alerts are part of the new and enhanced measures to protect consumers in Canada's Financial Consumer Protection Framework" (Financial Consumer Agency of Canada, 2022) and include notification of low balance and upcoming bill payments. Why not apply this proactive approach elsewhere? The concept of AI for good should not be limited to the development of AI solutions for public good, such as applications that address health or environmental issues. As is the case with the banks, a wide variety of business can be mandated to include AI practices for social and individual good as part of their service offerings. Why not cap surge pricing on Uber or

the fees the company charges drivers? Why not make dynamic pricing illegal? Regulations of this sort can not only protect and benefit individuals but also foster innovation.

Corporate Social Responsibility

Initiatives for social good, particularly those that go beyond regulatory requirements, are incorporated into companies' corporate social responsibility (CSR) practices. CSR practices are viewed as being good for companies' bottom line as they enhance reputation and foster consumer preference and loyalty. CSR practices are not without criticism. The term 'greenwashing' refers to activities companies undertake to appear to be addressing environmental issues such as pollution and global warming while at best doing nothing and at worst deflecting attention from actively harmful practices. Similarly, the term bluewashing has been applied to "the malpractice of making unsubstantiated or misleading claims about, or implementing superficial measures in favour of, the ethical values and benefits of digital processes, products, services, or other solutions in order to appear more digitally ethical than one is" (Floridi, 2019, p.187). For socially responsible digital practices that go beyond regulation to succeed:

> "Public, accountable, and evidence-based transparency about good practices and ethical claims should be a priority on the side of the actors wishing to avoid the appearance of engaging in any bluewashing malpractice. Public and factual education, on the side of any target of bluewashing—not just the general public but also members of executive boards and advisory councils, for example—about whether and what effective ethical practices are actually implemented means that actors may be less likely to (be tempted to) distract public attention away from the ethical challenges they are facing" (ibid, p. 188).

This study indicates that at least one bank has begun to consider data practices in the context of CSR and that this approach encourages companies and their employees to take a broader view of the potential harms and benefits inherent in their data practices.

This emerging practice area has also been dubbed "Corporate Digital Responsibility" (Lobschat et al., 2021; Herden et al, 2019). Corporate Digital Responsibility can be applied to a wide variety of impacts and potential harms beyond existing environmental and diversity and inclusion initiatives. For example, companies can support credible news sources or take a stand against AI generated content via commitments to how they invest advertising dollars. Labour disruption due to AI automation could be addressed via investments in retraining or supporting new educational initiatives.

Further Research

This thesis opens four avenues of further research:

1. As a benchmark prior to AI specific legislation in Canada, this study could be repeated in whole or part once new legislation is in place, allowing us to track how disclosures about the use of AI at the banks evolve. Given the results of the Wulf and Siezov study showing only 57% of AI disclosures meet current GDRP requirements, ongoing research on AI disclosures is a critical area of study.
2. This study could be expanded to include promotional material about AI produced by the banks such as press releases, white papers, and reports. The relative volume of and difference in tone between regulated and unregulated discourse could also be studied in relation to its impact on public understanding of and attitudes towards AI in banking.

3. Research could also be expanded to include consumer facing fintech companies such as Mint and Hardbacon. An examination of the discourse of these digital first companies is relevant given fintech is expected to grow by 36% in Canada in 2024 (Stastica, 2023) and is lobbying for open banking in Canada (Fintechs Canada, 2022).
4. This study could also be repeated for other sectors, such as retail (Canadian Tire, Loblaws, Sobeys, SportsChek, and so on) or telecommunications (Rogers, Bell, Shaw and Telus).

REFERENCES

Albu, O. B., & Flyverbom, M. (2019). Organizational Transparency: Conceptualizations, Conditions, and Consequences. *Business & Society*, *58*(2), 268–297. https://doi.org/10.1177/0007650316659851

Alloa, E. (2019). Transparency: a magical concept of modernity. In *Transparency, society and subjectivity: critical perspectives* (pp. 21–56). essay, Palgrave Macmillan.

Ananny, M. (2016). Toward an Ethics of Algorithms: Convening, Observation, Probability, and Timeliness. Science, Technology, & Human Values, 41 (1), pp. 93–117. doi:10.1177/0162243915606523.

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. New Media & Society, 20(3), 973-989. https://doi.org/10.1177/1461444816676645

Biswas, S., Carson, B., Chung, V., Singh, S., & Thomas, R. (2020, September 19). AI-Bank of the future: Can banks meet the AI challenge? McKinsey & Company. Retrieved April 15, 2023, from https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge

BMO. (2021, September 2). BMO Harnesses AI technology for capital markets structured note pricing and scenario analysis. About BMO . Retrieved April 15, 2023, from https://newsroom.bmo.com/2021-09-02-BMO-Harnesses-AI-Technology-for-Capital-Markets-Structured-Note-Pricing-and-Scenario-Analysis

Bourne. (2020). Fintech's Transparency–Publicity Nexus: Value Cocreation Through Transparency Discourses in Business-to-Business Digital Marketing. The American Behavioral Scientist (Beverly Hills), 64(11), 1607–1626. https://doi.org/10.1177/0002764220959385

Brandeis, L. (1913). *Other People's Money and the how the bankers use it.* The McClure Publications. Retrieved from http://www.gutenberg.org/files/57819/57819-h/57819-h.htm

Brandtzaeg, P. B., Pultier, A., & Moen, G. M. (2019). Losing Control to Data-Hungry Apps: A Mixed-Methods Approach to Mobile App Privacy. Social Science Computer Review, 37(4), 466–488. https://doi.org/10.1177/0894439318777706

Bruening, P. and Culnan, M.J. (2015) Through a Glass Darkly: From Privacy Notices to Effective Transparency. North Carolina Journal of Law and Technology, 17(4), pp. 515–580 Available at SSRN: https://ssrn.com/abstract=2654469

Buolamwini, J., & Gebru, T. (2018). Gender shades. Retrieved March 17, 2023, from http://gendershades.org/overview.html

Campbell-Verduyn, M., Goguen, M., & Porter, T. (2016). Big Data and Algorithmic Governance: The case of financial practices. New Political Economy, 22(2), 219–236.

Canada, G. of. (n.d.). *Fact sheet: Digital charter implementation act, 2020* [Landing Pages]. Retrieved April 12, 2021, from https://www.ic.gc.ca/eic/site/062.nsf/eng/00119.html

Canada, H. (2004, September 28). *Requirements for informed consent documents* [Backgrounders;guidance]. Gcnws. https://www.canada.ca/en/health-

canada/services/science-research/science-advice-decision-making/research-ethics-board/requirements-informed-consent-documents.html

Canadian Bankers Association. (2023, March 14). Focus: Fast Facts about the Canadian banking system. Canadian Bankers Association. Retrieved April 14, 2023, from https://cba.ca/fast-facts-the-canadian-banking-system

Caron, M. S. (2019). The Transformative Effect of AI on the Banking Industry. Banking & Finance Law Review, 34(2), 169-214. https://ezproxy.library.yorku.ca/login?url=https://www-proquest-com.ezproxy.library.yorku.ca/scholarly-journals/transformative-effect-ai-on-banking-industry/docview/2207836906/se-2?accountid=15182

CFI Team. (2022, December 5). Hirevue Interview Guide. Corporate Finance Institute. Retrieved April 15, 2023, from https://corporatefinanceinstitute.com/resources/career/about-hirevue-interview/

Chakrabarty, B., Seetharaman, A., Swanson, Z., & Wang, X. (Frank). (2018). Management Risk Incentives and the Readability of Corporate Disclosures. Financial Management, 47(3), 583–616. https://doi.org/10.1111/fima.12202

Christensen, L. T., & Cheney, G. (2015). Peering into transparency: Challenging ideals, proxies, and organizational practices. Communication Theory, 25(1), 70-90. https://doi.org/10.1111/comt.12052

Christensen, L. T., & Cornelissen, J. (2015). Organizational transparency as myth and metaphor. European Journal of Social Theory, 18(2), 132–149. https://doi.org/10.1177/1368431014555256

Citron, & Pasquale, F. A. (2014). The scored society: due process for automated predictions. Washington Law Review, 89(1), 1–33.

Colander, Goldberg, M., Haas, A., Juselius, K., Kirman, A., Lux, T., & Sloth, B. (2009). THE FINANCIAL CRISIS AND THE SYSTEMIC FAILURE OF THE ECONOMICS PROFESSION. Critical Review (New York, N.Y.), 21(2-3), 249–267. https://doi.org/10.1080/08913810902934109

Collie, F. (2021, February 24). How banks are harnessing artificial intelligence. Investment Executive. Retrieved April 15, 2023, from https://www.investmentexecutive.com/newspaper_/building-your-business-newspaper/how-banks-are-harnessing-artificial-intelligence/

Coulton, M. (2023, March 30). Canada godfather of AI calls for pause on technology he helped create. Financial Post. https://financialpost.com/technology/canadian-godfather-ai-pause-technology-helped-create

Crain. (2018). The limits of transparency: Data brokers and commodification. New Media & Society, 20(1), 88–104. https://doi.org/10.1177/1461444816657096

Crawford, K. (2021). The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. Yale University Press. https://doi.org/10.2307/j.ctv1ghv45t

Crotty, J. (2009). Structural causes of the global financial crisis: a critical assessment of the 'new financial architecture.' Cambridge Journal of Economics, 33(4), 563–580. https://doi.org/10.1093/cje/bep023

Cucciniello, M., Porumbescu, G. A., & Grimmelikhuijsen, S. (2016). 25 Years of Transparency Research: Evidence and Future Directions. *Public Administration Review*, *77*(1), 32–44. https://doi.org/10.1111/puar.12685

Das, G., Cheung, C., Nebeker, C., Bietz, M., & Bloss, C. (2018). Privacy policies for apps targeted toward youth: Descriptive analysis of readability. JMIR mHealth and uHealth, 6(1), e3-e3. https://doi.org/10.2196/mhealth.7626

De Cooman, J. (2022). Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act. Market and Competition Law Review, VI(1), 49–88. https://doi.org/10.34632/mclawreview.2022.11304

Drage, E., & Mackereth, K. (2022). Does AI debias recruitment? race, gender, and AIs "Eradication of difference." Philosophy & Technology, 35(4). https://doi.org/10.1007/s13347-022-00543-1

ECNL. (2021, March 23). *Evaluating the risk of AI systems to human rights from a tier-based approach*. European Center for Not For Profit Law. Retrieved April 15, 2023, from https://ecnl.org/news/evaluating-risk-ai-systems-human-rights-tier-based-approach

Eloundou, T., Manning, S., Mishkin, P., & Rock, D. (2023). GPTs and GPTs: An Early Look at the Labor Market Impact Potential of Large Language Models. Working Paper. https://doi.org/https://arxiv.org/pdf/2303.10130pdf

Encyclopædia Britannica, inc. (n.d.). Myth. Encyclopædia Britannica. https://www.britannica.com/topic/myth.

Etzioni, A. (2010). Is transparency the best disinfectant? The Journal of Political Philosophy, 18(4), 389-404. https://doi.org/10.1111/j.1467-9760.2010.00366

Etzioni, A. (2019). The Limits of Transparency. In *Transparency, society and subjectivity: critical perspectives* (pp. 179–201). essay, Palgrave Macmillan.

Evident Insights. (n.d.). About Us. Evident Insights. Retrieved April 15, 2023, from https://www.evidentinsights.com/about-us/

Fenster, M. (2015). Transparency in search of a theory. European Journal of Social Theory, 18(2), 150–167. https://doi.org/10.1177/1368431014555257

Financial Consumer Agency of Canada. (2022, June 30). *New electronic alerts from your bank*. Canada.ca. Retrieved March 17, 2023, from https://www.canada.ca/en/financial-consumer-agency/services/banking/new-electronic-alerts-banks.html

Financial Consumer Agency of Canada. (2021, October 29). *Government of Canada*. 2021 to 2026 Strategic Plan: Financial Consumer Agency of Canada - Canada.ca. Retrieved March 9, 2023, from https://www.canada.ca/en/financial-consumer-agency/corporate/planning/strategic-plans/strategic-plan-2021-2026.html

Financial Consumer Agency of Canada. (2022, June 30). Government of Canada. Canada.ca. Retrieved April 14, 2023, from https://www.canada.ca/en/financial-consumer-agency/services/banking/rights-new-protections.html

Fintechs Canada. (2022, December 1). About. Fintechs Canada. Retrieved April 15, 2023, from https://fintechscanada.ca/about/

Fitzgerald, M. (2021, January 28). *Robinhood restricts trading in GameStop, other names involved in frenzy*. CNBC. Retrieved March 9, 2023, from https://www.cnbc.com/2021/01/28/robinhood-interactive-brokers-restrict-trading-in-gamestop-s.html

Flesch, R. (1949). The art of readable writing. Harper.

Floridi, L. (2019). Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical. *Philosophy & Technology*, *32*(2), 185–193. https://doi.org/10.1007/s13347-019-00354-x

Flyverbom, M. (2015). Sunlight in cyberspace? On transparency as a form of ordering. European Journal of Social Theory, 18(2), 168–184. https://doi.org/10.1177/1368431014555258

Flyverbom, M. (2019). *The Digital Prism: Transparency and Managed Visibility in a Datafied World*. Cambridge University Press

Flyverbom, M., Christensen, L. T., & Hansen, H. K. (2015). The Transparency–Power nexus: Observational and regularizing control. Management Communication Quarterly, 29(3), 385-410. https://doi.org/10.1177/0893318915593116

Forssbæck, J., & Oxelheim, L. (2014). The Multifaceted Concept of Transparency. In *The Oxford Handbook of Economic and Institutional Transparency* (1st ed.). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199917693.013.0001

Fowler, L., Gillard, C., & Morain, S. (2020). Readability and Accessibility of Terms of Service and Privacy Policies for Menstruation-Tracking Smartphone Applications. Health Promotion Practice, 21(5), 679–683. https://doi.org/10.1177/1524839919899924

Friginal, E., Hardy, J. A., & Mautner, G. (2021). Business Discourse. In The Routledge Handbook of Corpus Approaches to discourse analysis (pp. 319–333). essay, Routledge.

Frischmann, & Selinger, E. (2018). Re-engineering humanity. Cambridge University Press.

Galaski, R. (2021, June 3). A roadmap to responsible innovation with AI in Financial Services. Deloitte Canada. Retrieved April 15, 2023, from https://www2.deloitte.com/ca/en/pages/financial-services/articles/navigating-unchartered-waters.html

Gee, Handford, M. & Smart, G. (2012). Discourse-oriented ethnography. In The Routledge handbook of discourse analysis (pp.147-159). essay, Routledge

Globe Editorial Board. (2023, April 5). *Globe editorial: The Robots Are Coming. Is Ottawa ready?* The Globe and Mail. Retrieved April 11, 2023, from https://www.theglobeandmail.com/opinion/editorials/article-the-robots-are-coming-is-ottawa-ready/

Goodyear, S. (2023, May 4). The "godfather of ai" says he's worried about "the end of people" | CBC radio. CBCnews. https://www.cbc.ca/radio/asithappens/geoffrey-hinton-artificial-intelligence-advancement-concerns-1.6830857

Gossett, S. (2023, March 13). *15 AI in banking examples you should know*. Built In. Retrieved April 12, 2023, from https://builtin.com/artificial-intelligence/ai-in-banking

Government of Canada. (2023, March 13). *Bill C-27 summary: Digital Charter Implementation Act, 2022*. Government of Canada. Retrieved March 17, 2023, from https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world

Granger, A. (2017, August 1). Banking in Canada. The Canadian Encyclopedia. Retrieved April 14, 2023, from https://www.thecanadianencyclopedia.ca/en/article/banking

Grundy, Chiu, K., Held, F., Continella, A., Bero, L., & Holz, R. (2019). Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. BMJ (Online), 364, l920–l920. https://doi.org/10.1136/bmj.l920

Heald, D. (2006). Transparency as an Instrumental Value. In *Transparency: the key to better governance?* (pp. 59–73). Oxford University Press.

Heald, D. (2006). Varieties of Transparency. *In Transparency: the key to better governance?* (pp. 25–43). Oxford University Press.

Heaven, W. D. (2020, December 10). *Predictive policing algorithms are racist. they need to be dismantled.* MIT Technology Review. Retrieved March 17, 2023, from https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/

Hentzen, Hoffmann, A., Dolan, R., & Pala, E. (2022). Artificial intelligence in customer-facing financial services: a systematic literature review and agenda for future research. International Journal of Bank Marketing, 40(6), 1299–1336. https://doi.org/10.1108/IJBM-09-2021-0417

Herden, C., Alliu, E., Cakici, A., Cormier, T., Deguelle, C., Gambhir, S., Griffiths, C., Gupta, S., Kamani, S., Kiratli, Y., Kispataki, M., Lange, G., Moles de Matos, L., Tripero Moreno, L., Betancourt Nunez, H., Pilla, V., Raj, B., Roe, J., Skoda, M., Edinger-Schons, L. (2021). Corporate Digital Responsibility: New corporate responsibilities in the digital age. *Sustainability Management Forum|NachhaltigkeitsManagementForum*. https://doi.org/10.1007/s00550-020-00509-x

Hildebrand, & Bergner, A. (2021). Conversational robo advisors as surrogates of trust: onboarding experience, firm perception, and consumer financial decision making. Journal of the Academy of Marketing Science, 49(4), 659–676. https://doi.org/10.1007/s11747-020-00753-z

Hitlin, & Rainie, L. (2019). Facebook Algorithms and Personal Data. In Policy File. Pew Research Center.

Holton, G.A. (2002). History of Value-at-Risk: 1922-1998.

Hong, S. (2020). *Technologies of speculation: the limits of knowledge in a data-driven society*. New York University Press.

Huckvale, Torous, J., & Larsen, M. E. (2019). Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. JAMA Network Open, 2(4), e192542–e192542. https://doi.org/10.1001/jamanetworkopen.2019.2542

Ibáñez, & Olmeda, M. V. (2022). Operationalising AI ethics: how are companies bridging the gap between practice and principles? An exploratory study. AI & Society, 37(4), 1663–1687. https://doi.org/10.1007/s00146-021-01267-0

Ibiricu, B., & van der Made, M. (2020). Ethics by design: a code of ethics for the digital age. *Records Management Journal (London, England), 30* (3), pp.395–414. https://doi.org/10.1108/RMJ-08-2019-0044

IFRS home. IFRS. (n.d.). Retrieved August 23, 2022, from https://www.ifrs.org/about-us/who-we-are/

Innovation, Science and Economic Development Canada. (2023, March 13). *The Artificial Intelligence and Data Act (AIDA) – Companion document*. Innovation, Science and Economic Development Canada Main Site . Retrieved April 17, 2023, from https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s5

Jaggi, P. (2023, February 21). Revolutionize your banking processes with Intelligent Document Processing (IDP). Parashift. Retrieved April 15, 2023, from https://parashift.io/en/revolutionise-banking-processes-with-intelligent-document-processing/

Jaworska. (2018). Change But no Climate Change: Discourses of Climate Change in Corporate Social Responsibility Reporting in the Oil Industry. International Journal of Business Communication (Thousand Oaks, Calif.), 55(2), 194–219. https://doi.org/10.1177/2329488417753951

Kara, S. (2023) Cobalt Red: How the blood of the Congo powers our lives. St. Martin's Press

Kaye, K. (2021, April 28). Senators want more transparency into social media algorithms. Digiday. https://digiday.com/media/cheat-sheet-senators-want-more-transparency-into-addictive-facebook-twitter-and-youtube-algorithms/.

Kear, M. (2017). Playing the credit score game: Algorithms, 'positive' data and the personification of financial objects. Economy and Society, 46(3-4), 346–368. https://doi.org/10.1080/03085147.2017.1412642

Kitchin, Rob. 2017. "Thinking Critically about and Researching Algorithms." Information, Communication & Society 20(1):14–29.

Krych, & McDaniel, P. (2021). Exposing Android social applications: linking data leakage to privacy policies. Journal of Cyber Security, 5(3-4), 139–190. https://doi.org/10.1080/23742917.2019.1630093

Lauer, Josh. Creditworthy: A History of Consumer Surveillance and Financial Identity in America, New York Chichester, West Sussex: Columbia University Press, 2017. https://doi-org.ezproxy.library.yorku.ca/10.7312/laue16808

Leufer, D., & Hidvegi, F. (2022, January 25). *The EU should regulate AI on the basis of rights, not risks*. Access Now. Retrieved March 12, 2023, from https://www.accessnow.org/eu-regulation-ai-risk-based-approach/

Lexico Dictionaries. (n.d.). *ASSUMPTION: Definition of ASSUMPTION by Oxford Dictionary on Lexico.com*. Lexico Dictionaries | English. https://www.lexico.com/definition/assumption.

Lexico Dictionaries. (n.d.). *MYTH: Definition of MYTH by Oxford Dictionary on Lexico.com also meaning of MYTH*. Lexico Dictionaries | English. https://www.lexico.com/definition/myth.

Li, Y., Stewart, W., Zhu, J., Ni, A., & Rohm, C. (2012). Online privacy policy of the thirty Dow Jones Corporations: compliance with FTC Fair Information Practice Principles and readability assessment. *Communications of the IIMA*, *12*(3), 65–.

Lightstone, & Driscoll, C. (2008). Disclosing elements of disclosure: a test of legitimacy theory and company ethics. Canadian Journal of Administrative Sciences, 25(1), 7–21. https://doi.org/10.1002/cjas.50

Lobschat L., Mueller B., Eggers F., Brandimarte, L., Diefenbach, S., Kroschke, M., Wirtz, J. (2021) Corporate Digital Responsibility. *Journal of Business Research*, 122, pp. 875-888, https://doi.org/10.1016/j.jbusres.2019.10.006.

Macklem, T., Rogers, C., Lane, T., Schembri, L., Beaudry, P., Gravelle, T., & Koziki, S. (2022, June 9). Financial system review-2022. Bank of Canada. Retrieved April 15, 2023, from https://www.bankofcanada.ca/2022/06/financial-system-review-2022/#cyber-security

Martin. (2015). Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online. Journal of Public Policy & Marketing, 34(2), 210–227. https://doi.org/10.1509/jppm.14.139

Martins, Gomes, D., & Manuel Castelo Branco. (2021). Managing Corporate Social and Environmental Disclosure: An Accountability vs. Impression Management Framework. Sustainability (Basel, Switzerland), 13(1), 296–. https://doi.org/10.3390/su13010296

Maurer, T., & Nelson, A. (n.d.). *The global cyber threat to financial systems – IMF F&D*. IMF. Retrieved March 9, 2023, from https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

McClanahan, A. (2018). Dead pledges: Debt, crisis, and twenty-first -century culture. STANFORD University Press.

Mengotto, M. (2023, April 5). *Why financial institutions are banking on ai*. CIO. Retrieved April 12, 2023, from https://www.cio.com/article/472323/why-financial-institutions-are-banking-on-ai.html#:~:text=Banks%20have%20been%20able%20to,with%20AML%20and%20KYC%20requirements

Mordor Intelligence. (n.d.). Algorithmic trading market trends. Mordor Intelligence. Retrieved April 15, 2023, from https://www.mordorintelligence.com/industry-reports/algorithmic-trading-market/market-trends Nalbandian, L. (2021, April 29). Canada should be transparent in how it uses AI to screen immigrants. The Conversation. https://theconversation.com/canada-should-be-transparent-in-how-it-uses-ai-to-screen-immigrants-157841.

Mousavizadeh, A., & Ayles, A. (2023, January). Evident AI Index Banks. Evident Insights. Retrieved April 15, 2023, from https://www.evidentinsights.com/reports/evident-ai-index-for-banks-key-findings-report/?id=01a83e42db

Noble, Safiya Umoja. (2018). Algorithms of Oppression: How Search Engines Reinforce Racism. New York: New York University Press

Obar, J. A. (2019). The Data Privacy Transparency of Canadian Internet Carriers: A Third Report. York University

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 23(1), 128-147.

Obar, J. A. (2022). Unpacking “the biggest lie on the internet”: Assessing the length of terms of service and privacy policies for 70 Digital Services. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4293363

Office of the Privacy Commissioner of Canada. (2021, August 13). Guidelines for obtaining meaningful consent. Office of the Privacy Commissioner of Canada. Retrieved March 17, 2023, from https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

Office of the Superintendent of Financial Institutions. (2014, February 4). *Guide to intervention for federally regulated deposit-taking institutions*. Office of the Superintendent of Financial Institutions. Retrieved March 9, 2023, from https://www.osfi-bsif.gc.ca/Eng/fi-if/rai-eri/sp-ps/Pages/gid.aspx

Office of the Superintendent of Financial Institutions. (2021, December 23). Enterprise-wide model risk management for deposit-taking institutions. Office of the Superintendent of Financial Institutions. Retrieved August 23, 2022, from https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/e23.aspx

Office of the Superintendent of Financial Institutions. (2022, May 20). *Proposed revisions to Guideline E-23 on model risk management*. Office of the Superintendent of Financial Institutions. Retrieved March 9, 2023, from https://www.osfi-bsif.gc.ca/Eng/fi-if/in-ai/Pages/E-23_let.aspx

Office of the Superintendent of Financial Institutions. (2023, April 17). Financial Industry Forum on Artificial Intelligence: A Canadian perspective on responsible AI. Office of the Superintendent

of Financial Institutions. Retrieved April 18, 2023, from https://www.osfi-bsif.gc.ca/Eng/osfi-bsif/rep-rap/Pages/ai-ia.aspx

O'Neil, C. (2016). Weapons of math destruction. Broadway Books.

Parliament of Canada. (n.d.). *Government Bill (House of Commons) C-27 (44-1) - first reading ...* Retrieved March 10, 2023, from https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

Park, Y., Chung, J., & Shin, D. (2018). The Structuration of Digital Ecosystem, Privacy, and Big Data Intelligence. *The American Behavioral Scientist*, 62(10), pp.1319–1337. https://doi.org/10.1177/0002764218787863

Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

Payette, & Torrie, V. (2020). AI Governance in Canadian Banking: Fairness, Credit Models, and Equality Rights. Banking & Finance Law Review, 36(1), 5–38.

Qian, Y. (2020). A critical genre analysis of MD&A discourse in corporate annual reports. Discourse & Communication, 14(4), 424–437. https://doi.org/10.1177/1750481320910525

Rice, M., & Bogdanov, E. (2019). Privacy in Doubt: An Empirical Investigation of Canadians' Knowledge of Corporate Data Collection and Usage Practices. *Canadian Journal of Administrative Sciences*, *36*(2), 163–176. https://doi.org/10.1002/cjas.1494

Saltz, J. S., & Dewar, N. (2019). Data science ethical considerations: A systematic literature review and proposed project framework. *Ethics and Information Technology, 21*(3), pp.197-208. doi:http://dx.doi.org.ezproxy.library.yorku.ca/10.1007/s10676-019-09502-5

Schembri , L., & Globerman, S. (2023, January 11). *Opinion: The Bank of Canada still lags in transparency*. Financial Post. Retrieved March 17, 2023, from https://financialpost.com/opinion/bank-of-canada-transparency

Schnackenberg, A. K., & Tomlinson, E. C. (2016). Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships. Journal of Management, 42(7), 1784–1810. https://doi.org/10.1177/0149206314525202

Scotiabank. (2021, November 25). Scotiabank wins best AI initiative award from the Digital Banker. Perspectives. Retrieved April 15, 2023, from https://www.scotiabank.com/ca/en/about/perspectives.articles.impact.2021-11-scotiabank-recognized-best-ai-initiative-by-digital-banker.html

Seaver, Nick. (2017). "Algorithms as Culture: Some Tactics for the Ethnography of Algorithmic Systems." Big Data & Society 4(2):1–12.

Shanmuganathan, M. (2020). Behavioural finance in an era of artificial intelligence: Longitudinal case study of robo-advisors in investment decisions. Journal of Behavioral and Experimental Finance, 27, 100297–. https://doi.org/10.1016/j.jbef.2020.100297

Soldatos, J., & Kyriazis, D. P. (2022). Big data and artificial intelligence in digital finance : increasing personalization and trust in digital finance using big data and AI (Soldatos & D. P. Kyriazis, Eds.). Springer International Publishing AG.

Solomon, H. (2021, May 29). *Two Canadian banks could pay up to $23 million to settle lawsuits in 2018 hacks: It world canada news*. IT World Canada. Retrieved March 9, 2023, from https://www.itworldcanada.com/article/two-canadian-banks-could-pay-up-to-23-million-to-settle-lawsuits-in-2018-hacks/446673

Stahl, Antoniou, J., Ryan, M., Macnish, K., & Jiya, T. (2022). Organisational responses to the ethical issues of artificial intelligence. AI & Society, 37(1), 23–37. https://doi.org/10.1007/s00146-021-01148-6

Stastica. (2023, April). Fintech - Canada: Statista market forecast. Statista. Retrieved April 15, 2023, from https://www.statista.com/outlook/dmo/fintech/canada

Statistics Canada. (2022, October 18). *Impact of cybercrime on Canadian businesses, 2021*. The Daily - . Retrieved March 9, 2023, from https://www150.statcan.gc.ca/n1/daily-quotidien/221018/dq221018b-eng.htm

Stohl, C., Stohl, M., & Leonardi, P. M. (2016). Managing opacity: Information visibility and the paradox of transparency in the digital age. International Journal of Communication (Online), 10, 123 137.

TBS Report. (2023, January 22). *Good governance, transparency key to revive economy: Economists*. The Business Standard. Retrieved March 18, 2023, from https://www.tbsnews.net/bangladesh/good-governance-transparency-key-revive-economy-economists-571834

TD Bank Group. (2019, January 8). *TD integrates artificial intelligence-powered chatbot into its top-ranked mobile app*. Cision Canada. Retrieved April 15, 2023, from

https://www.newswire.ca/news-releases/td-integrates-artificial-intelligence-powered-chatbot-into-its-top-ranked-mobile-app-834588043.html

TD Bank Group. (2022, January 26). As fraudsters become more sophisticated, TD Insurance Expands Artificial Intelligence Fraud Prevention Program to better protect customers. TD Stories. Retrieved April 15, 2023, from https://stories.td.com/ca/en/news/2022-01-26-as-fraudsters-become-more-sophisticated-2c-td-insurance-expand

Td Easy Trade: Becoming an Investor. (2022). *YouTube*. Retrieved March 17, 2023, from https://youtu.be/oJRyaTaPFVk.

Tribunal, S. S. (2019, June 21). *Readability assessment: Appeals correspondence*. https://www1.canada.ca/en/sst/readability.html

Truby, Brown, R., & Dahdal, A. (2020). Banking on AI: mandating a proactive approach to AI regulation in the financial sector. Law and Financial Markets Review, 14(2), 110–120. https://doi.org/10.1080/17521440.2020.1760454

Turow, J., Hennessy, M., & Draper, N. (2018). Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003-2015. *Journal of Broadcasting & Electronic Media*, *62*(3), 461–478. https://doi.org/10.1080/08838151.2018.1451867

Verdegem, P., & Prodnik, J. (2021). Algorithmic Logic in Digital Capitalism. In AI for everyone?: Critical perspectives. essay, University of Westminster Press.

Waschuck & Hamilton (2022). *AI in the Canadian Financial Services Industry*. McCarthy Tétrault. Retrieved March 9, 2023, from https://www.mccarthy.ca/en/insights/blogs/techlex/ai-canadian-financial-services-industry

Wulf, & Seizov, O. (2022). “Please understand we cannot provide further information”: evaluating content and transparency of GDPR-mandated AI disclosures. AI & Society. https://doi.org/10.1007/s00146-022-01424-z

Yeung, K., Howes, A., & Pogrebna, G. (2022). AI Governance by Human Rights–Centered Design, Deliberation, and Oversight. In The Oxford Handbook of Ethics of AI. essay, Oxford University Press.

Yin, R. K. (2018). *Case study research and applications: design and methods*. SAGE.

Zhang M, Chow A, Smith H. (2020). COVID-19 Contact-Tracing Apps: Analysis of the Readability of Privacy Policies. J Med Internet Res 22(12). URL: https://www.jmir.org/2020/12/e21572. DOI: 10.2196/21572

Zook, & Spangler, I. (2023). A Crisis of Data? Transparency Practices and Infrastructures of Value in Data Broker Platforms. Annals of the American Association of Geographers, 113(1), 110–128. https://doi.org/10.1080/24694452.2022.2071201

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.