DATA-GATHERING, GOVERNANCE, AND ALGORITHMS: HOW ACCOUNTABLE AND TRANSPARENT PRACTICES CAN MITIGATE ALGORITHMIC THREATS

by

Alexander Gramegna

BA, University of Toronto, 2017

A Major Research Paper

presented to Ryerson University

in partial fulfillment of the

requirements for the degree of

Master of Professional Communication

Toronto, Ontario, Canada, 2018

AUTHOR'S DECLARATION

I hereby declare that I am the sole author of this MRP. This is a true copy of the MRP, including any required final revisions.

I authorize Ryerson University to lend this MRP to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this MRP by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my MRP may be made electronically available to the public.

DATA-GATHERING, GOVERNANCE, AND ALGORITHMS: HOW ACCOUNTABLE AND TRANSPARENT PRACTICES CAN MITIGATE ALGORITHMIC THREATS

© Alexander Gramegna

Master of Professional Communication, 2018

Ryerson University

ABSTRACT

Corporate use of algorithms for marketing purposes often entails that user data is collected and processed by corporations to influence consumers online. Despite the technological efficiencies that many algorithms provide, algorithms often pose threats to human autonomy and privacy in a consumer context. While algorithms have the capacity to influence individuals and shape their behaviour, human inputs and regulations shape their functions and mandates. Regulatory measures and government legislation are also capable of shaping algorithmic functions, sometimes in ways that mitigate threats to user autonomy and privacy. Many scholars suggest that implementing practices of accountability and transparency into algorithmic regulation can mitigate the threats algorithms pose to society. This Major Research Paper will conceptualize algorithmic threats to user privacy and autonomy, as well as practices of accountability and transparency. A critical analysis of the European Union's *General Data Protection Regulation* will assist in recognizing specific practices that are capable of mitigating algorithmic threats to user privacy and autonomy. The analysis and discussion of the GDPR's potential efficacy will use mutual shaping theory to explore the role legislation plays in the co-evolution of algorithmic technology and society.

Key Words: Algorithms, Data-Gathering, Privacy, Autonomy, Accountability, Transparency, General Data Protection Regulation, GDPR, European Union, Mutual Shaping Theory

ACKNOWLEDGEMENTS

I would like to thank and acknowledge my first reader, Dr. John Shiga, and second reader, Dr. Matthew Tiessen for their continued support. Their insight, feedback, and encouragement were instrumental in writing this Major Research Paper.

Table of Contents

Introduction

Many information technology and social media companies generate profits by taking advantage of user tracking, data gathering, and algorithms (West, 2017; Mager, 2012). Although many algorithms offer benefits to society (Flyverbom, Deibert, & Matten, 2017), some pose threats to users' privacy and autonomy (Doneda & Almeida, 2016). This MRP will focus on algorithms in a consumer context, where corporate actors amass databases of user information, then operationalize data through algorithms to influence the "decisional processes" of individuals (Doneda & Almeida, 2016). While there is potential for firms to regulate their own use of algorithms, many have failed to do so (West, 2017), and state involvement in regulating data-collection practices and algorithmic functions has been minimal in the past decade (Saurwein et al., 2015). However, as of May 2018, the European Union (EU) has put into effect its *General Data Protection Regulation* (GDPR), a ground-breaking piece of legislation that comprehensively regulates practices of data-collection, processing, and operationalization through algorithms. As legislation is created in response to algorithms and their threats, there is opportunity to analyze emerging forms of government regulation of algorithms.

Many scholars have identified a variety of threats that algorithms pose to society, and many have suggested that practices of accountability and transparency can mitigate or eliminate such threats (Mager, 2012; Doneda & Almeida, 2016; Gasser & Almeida, 2017; Just & Latzer, 2017). In this MRP, I will examine the algorithmic threats to user autonomy and privacy in a consumer context, and conceptualize practices of accountability and transparency in relation to corporate intent, algorithmic design, and processes of data-collection and operationalization. Through analysis of relevant literature, I find that corporate data-collection poses threats to privacy through a lack of accountability to users, while both data-collection and

operationalization via algorithms pose threats to autonomy through a lack of transparency and user awareness. Additionally, algorithmic design serves as a key variable in determining the effects that algorithms have on society. From there, I proceed to answer the following research questions:

RQ1: Can government legislation mitigate threats posed by corporate algorithm use?

RQ2: Can practices of transparency and accountability mitigate threats to user privacy and autonomy?

RQ3(a): How does regulating data-collection and processing shape algorithmic functions to mitigate algorithmic threats to user privacy and autonomy?

RQ3(b):How does the GDPR mitigate algorithmic threats through regulations that establish practices of accountability and transparency?

Research questions 1 and 2 will be addressed through the literature review as conceptualizations of algorithms, their threats, transparency, and accountability are developed in context with internet governance and consumer society. The literature review begins to answer research question 3(a) by drawing relationships between these conceptualizations, and the case of the GDPR serves as a contemporary example that illustrates how regulating data-collection can mitigate algorithmic threats. A critical analysis of specific policies in the GDPR will then answer research questions 3(b).

Overall, government legislation has the capacity to promote practices of transparency and accountability to diminish algorithmic threats to user autonomy and privacy. While there are various ways in which internet governance can shape algorithmic functions, I will use the GDPR as a case study to explore how government legislation can limit algorithmic threats by enforcing practices of transparency and accountability that align with conceptualizations outlined in the

literature review. The mutual shaping theory of technology and society provides a framework with which to analyze the relationship between algorithms, their threats, practices of accountability and transparency, and government legislation. According to mutual shaping theory, government legislation and algorithmic technology (including their data-centric inputs, corporate designs, and functions as outputs) continuously affect each other in a mutually constituted process. However, theories of technological determinism and social constructivism provide reasonable perspectives in analyzing the relationship between algorithmic technologies and society. The GDPR may be considered as a social constructionist response to algorithmic technologies that shape – and potentially threaten – society in ways that align with technological determinism. The GDPR indicates that there is potential for legislation to serve as a social force in shaping technology, but evaluating its theoretical effectiveness in limiting technological determination requires an analysis of how technology is capable of influencing society. Yet as society and technology continuously influence each other according to mutual shaping theory, there must be points where one can begin and end the analysis of how societal influences such as legislation can affect algorithmic technologies and vice versa. As I will focus on how practices of accountability and transparency can mitigate algorithmic threats through legislation, I will theoretically track how the GDPR uses such practices to empower social forces in shaping technology. The GDPR may empower social shaping of algorithmic technologies in ways that align with theories of social constructivism, but I will emphasize algorithmic technology's capacity to shape society in order to understand how legislation addresses technology's influence.

After analyzing the GDPR, the discussion on its potential effectiveness in mitigating algorithmic threats will be understood through the lens of mutual shaping theory. While the

practical effects of the GDPR on algorithmic functions and threats are important, the recent development and implementation of the GDPR prevents an empirical analysis of its impact on society. The common themes and concepts identified in the literature review will provide a methodological strategy to analyze the role of specific practices facilitated by the GDPR in mitigating algorithmic threats. Analyzing practices of algorithmic regulation in accordance with mutual shaping theory will identify how government legislation such as the GDPR can theoretically diminish algorithmic threats by enforcing corporate practices of transparency and accountability to regulate data-collection and operationalization. However, mutual shaping theory not only informs an understanding of regulatory efficacy, but also illustrates how technological developments can shape societal responses and the actions of policy makers.

Method of Analysis

To answer each research question and understand how legislation can mitigate algorithmic threats, the analysis of the literature and GDPR must consider the relationship between algorithmic functions and consumer society in line with mutual shaping theory. In brief summary, algorithmic technologies and consumer society develop in a mutually constituted fashion. Algorithms have the capacity to influence consumer behaviour, triggering societal and legislative responses that may limit or enhance their capabilities to influence consumption patterns. On the other hand, human inputs and legislation are each capable of shaping algorithmic functions as they determine algorithmic outputs and shape the scope of data-collection and processing respectively.

To answer research question one (*Can government legislation mitigate threats posed by corporate algorithm use?*), algorithms and their threats must be conceptualized in specific accordance with their role in consumer society, where they can serve to influence consumer

decision-making based on user data that is collected, stored, and processed to function according to corporate designs. To answer research question two (*Can practices of transparency and accountability mitigate threats to user privacy and autonomy?*), principles of accountability and transparency must be understood in the context of consumer society, and also conceptualized as practices that fulfill certain criteria as described in the scholarly literature, such as the creation of active information channels and protocols for control and oversight. To answer research question 3(a) (*How does regulating data-collection and processing shape algorithmic functions to mitigate algorithmic threats to user privacy and autonomy?*), I will theorize how regulation through government legislation can mitigate threats according to the mutual shaping theory. Finally, I will use the case of the GDPR to answer research question 3(b) (*How does the GDPR mitigate algorithmic threats through regulations that establish practices of accountability and transparency?*) by outlining how specific regulations may mitigate algorithmic threats as they establish transparent and accountable practices that align with previous conceptualizations.

The critical analysis of the GDPR will examine: 1) the specific practices of accountability and transparency established; 2) the role of such practices in shaping corporate intent, data-collection, as well as algorithmic design and functions, and; 3) the potential effectiveness of such practices in mitigating algorithmic threats to human autonomy and privacy, in accordance with the literature on each concept. The GDPR will be qualitatively analyzed to explore the extent to which practices of accountability and transparency are applied in government legislation to protect individuals from algorithmic threats. The analysis will determine if practices of accountability and transparency are capable of mitigating algorithmic threats by using mutual shaping theory to gauge their possible efficacy. In the discussion section, mutual shaping theory

can identify how legislation such as the GDPR serves as a social force to shape algorithmic functions and mitigate threats to human autonomy and privacy.

Conceptualizing Algorithms in a Consumer Context

Definitions of Algorithms

The notion of an algorithm can be understood in a number of contexts depending on its application. From a social science perspective, Quan-Haase (2013) defines an algorithm as "a problem solving method used in mathematics and computer science expressed in the form of a series of instructions" (p. 231). From a computer science perspective, Yanofksy (2011) informally defines an algorithm as "any well-defined computational procedure that takes some value, or set of values, as input and produces some value, or set of values, as output" (p. 253). More technically, Yanofsky's (2011) definition of an algorithm is dependent on the computational programming language used to develop the algorithm. However, algorithms are also shaped by social influences such as the biases and intentions of their creators since their outputs are dependent on human programming and user inputs (Foer, 2017). Additionally, the social impact of algorithms is dependent on their design, rather than on their technological nature (Cavoukian, 2009). By definition, an algorithm is a broad term that generally entails a sets of rules followed in process. Given the broad nature of algorithms, any study highlighting the effects that society and legislation may have on algorithmic functions and their potential threats must identify the specific context and application of the type of algorithm in discussion.

Gal and Elkin-Koren (2017) conceptualize algorithms in a contemporary context of consumerism and e-commerce. According to their definition, algorithms are "structured decision-making processes that employ a set of rules or procedures, such as a decision tree, to automatically supply outcomes based on data inputs and decisional parameters" (Gal & Elkin-

Koren, 2017, p. 313). While their definition of algorithms is similar to others as they highlight their functional capabilities, it is unique as it emphasizes how corporate applications of algorithms create efficiencies in market operations. Furthermore, the authors highlight how advanced applications of algorithms use machine learning, a process by which an algorithm "learns from its own analyses of previous data how to refine and redefine its decision parameters" (Gal & Elkin-Koren, 2017, p. 313). Between machine learning and the collection of user data to determine behavioural patterns across consumer society, the increased technological capabilities of algorithms may create implications for policy makers as the technology can affect society in new ways.

Gal & Elkin-Koren's conceptualization of algorithms outlines their potential effects on consumers in accordance with mutual shaping theory, especially as algorithms "help consumers make decisions in market transactions" (Gal & Elkin-Koren, 2017, p. 314). As I will use mutual shaping theory to understand how corporate algorithms affect society and vice versa, my conceptualization of algorithms will align with Gal & Elkin-Koren's. My conceptualization of algorithms will specifically refer to computational processes employed by corporate actors, which require the collection of user data to influence consumer behaviour. I will use mutual shaping theory to explore the potential effects of government legislation on perceived algorithmic threats to human autonomy and privacy, while also using the theory to understand how algorithms are applied to corporate practices to shape consumer society to a certain extent. Considering that algorithms can shape consumer behaviour and government responses, while government legislation and social perspectives can shape algorithmic functions and corporate actions, my conceptualization of algorithms will also highlight the interplay of society and technology.

The Social Shaping of Algorithmic Functions

Assessing the relevance of algorithmic functions demonstrates that they have a significant influence on consumer behaviour. Identifying the role algorithmic functions have in consumers' day-to-day life provides grounds for later identifying their capacity to threaten the privacy and autonomy of individuals that interact with them. Gal and Elkin-Koren (2017) coin the term "algorithmic consumers," which are algorithms that can act on behalf of individuals for certain purchases in a process of "using data to predict consumers' preferences, choosing the products or services to purchase, [and] negotiating and executing the transaction" (Gal & Elkin-Koren, 2017, p. 310). Although some researchers predict that algorithmic consumers will be central actors in "the next generation of e-commerce," algorithmic applications also have the capacity to bypass human decision-making in many circumstances, ultimately transforming the way consumers interact with markets (Gal & Elkin-Koren, 2017). In a consumer context, algorithmic applications are promoted (or justified) on the grounds that they offer utilities by allowing individuals to compare products based on price and quality to make quicker and better-informed choices when shopping across markets (Gal & Elkin-Koren, 2017). Nevertheless, algorithms can intervene in "the subjective choices of individual users" and bypass consumer inputs, especially considering the possibilities of machine learning (Gal & Elkin-Koren, 2017, p. 311-2). As algorithms have the capability to create scenarios capable of influencing consumer decision-making and play a greater role in the market, the relevance of algorithmic functions in a consumer context provides reason to consider the potential threats their influence may pose to human autonomy and privacy.

While algorithms are capable of influencing consumer decision-making, their capacity to do this is dependent on their inputs as their function is facilitated and constrained by their design. For instance, algorithms do not inherently influence consumer decisions, but are rather designed with that specific capability in mind (Cavoukian, 2009; Gal and Elkin-Koren, 2017; Vedder & Naudts, 2017). Because algorithms are human constructs, they embody the values of their creators with their function being affected by the intentions and goals of their creators (Vedder & Naudts, 2017). Furthermore, algorithms are contextually dependent since they "are developed as part of a corporate culture, being produced by teams" and given particular mandates (Vedder & Naudts, 2017, p. 210). In assessing the social shaping of algorithmic functions, it is essential to consider the human influences apparent in algorithmic design as they will later determine the potential threats algorithms may pose to human autonomy and privacy. And while the intention of algorithmic design serves as an input that affects algorithmic function, consumer data also serves as an input that shapes algorithmic outputs. In and of themselves, algorithms are "inert and without meaning; they need to be paired with databases" since they operate as part of a larger computational structure (Vedder & Naudts, 2017, p. 209). Assessing the social shaping of algorithmic functions in a consumer context, then, also requires an exploration of the role of data as an algorithmic input that shapes its functions.

Vedder and Naudts (2017) note that algorithmic functions rely on the collection and processing of user data as they affect individuals "based on how the data suggest they might behave or should behave on the basis of patterns in the past, rather than based on the actual behaviour of the individuals" (p. 209). By examining how and where algorithms are utilized, the context of algorithmic use can help assess algorithmic accountability to users (Vedder & Naudts, 2017, p. 209). In other words, algorithmic effects are not solely a function of their technical

code; these effects are also based on the environments they operate in, particularly because data as an input dictates how algorithms function and who they affect. Consumer data, corporate intent, and human design all serve as algorithmic inputs that affect algorithmic outputs and functions. Exploring how such dependencies affect notions of algorithmic transparency and accountability will be discussed in later sections, but for now it should be noted that these dependencies shape the way algorithms function in a consumer context. Furthermore, my conceptualization of algorithms emphasizes the functional dependency of key inputs. Understanding the way legislation can shape algorithmic functions therefore also entails an analysis of how government regulation shapes algorithmic inputs such as data collection practices and corporate intent.

Data as an Algorithmic Input

A key input in informing an algorithm's instructional process is the collection of user data. Algorithms often process data gathered at a previous point in time to determine patterns and trends in consumer behaviour (Vedder & Naudts, 2017). Typically, user data is collected when users voluntarily provide personal information online, or when their activity online is monitored (Mager, 2012, West, 2017). Therefore, it is important to conceptualize data as a necessary requirement that shapes algorithmic outputs and the capability of their functions. The multitude of user information and browsing activity that is given to organizations as users shop online and surf the web makes data a valuable but cheap commodity (Haque, 2015). Data-mining practices involve methodological techniques where computer software is used in the process of "discovering meaningful correlations, patterns and trends by sifting through large amounts of data stored in repositories" (Haque, 2015). The mass of data collected through the internet

enables online organizations to create detailed behavioural profiles used meet the organization's goals, typically to market a product or service to a targeted audience (Haque, 2015). To give one example, Haque (2015) explains how Google's privacy policy in 2012 permitted them to collect and share user data as they utilized their products and services. These data collection practices enable companies to understand consumer behaviour patterns to anticipate future behaviour and manipulate it according to their goals (Haque, 2015). In many cases, this data is used as an algorithmic input and is operationalized to create outputs that are designed to influence consumer behaviour online. Targeted advertising of a particular product or service is a typical example of how many organizations market to users whose data profile suits their product or service (West, 2017).

As data-collection enables targeted marketing, algorithmic inputs are generated by societal actors and used to influence their behaviour through algorithmic outputs in a constant cycle of shaping. Gal and Elkin-Koren (2017) outline the four stages of the "algorithmic consumer," with the first two identifying the role of user data as a key input in this process. The first stage is the collection of user data, typically through "sensors" or online tracking of user browsing activity online (Gal & Elkin-Koren, 2017). The second stage is "data analytics", which entails that an algorithm analyses the user's personal data to discern an individual's consumption patterns, preferences, and purchase options (Gal & Elkin-Koren, 2017). In the specific context of the algorithmic consumer, the third stage involves the algorithm's data analysis informing a purchasing decision, whereas the fourth stage involves the actual purchasing of the product on behalf of the consumer (Gal & Elkin-Koren, 2017). Even outside of the context of algorithmic consumers, the first two steps identify how algorithms function based on the collection and analysis of user data.

Algorithms and Threats to Society

The Importance of Algorithmic Design

Algorithms do not inherently pose threats to society, but many algorithms with corporate designs pose threats to human autonomy and privacy. Any threat posed by algorithmic technology is not a result of the algorithm's functions or capabilities, but rather the design and application of the algorithm (Gal and Elkin-Koren, 2017; Cavoukian, 2009). In fact, algorithms offer benefits and efficiencies to both businesses and consumer as they "reduce information and transaction costs" and speed up decision-making processes based on their "analytical sophistication" (Gal & Elkin-Koren, 2017, p. 318-20). Moreover, algorithms are also capable of overcoming consumer biases and "manipulative marketing techniques, which play upon people's insecurities, frailties, unconscious fears, aggressive feelings and sexual desires to alter their thinking, emotions and behaviour" (Gal & Elkin Koren, 2017, p. 321). Considering the virtues of algorithmic technology, one may question how they could both overcome manipulation and further it. Just as algorithms are "inert and without meaning" (Vedder & Naudts, 2017), their design and specific application can either serve to further manipulative marketing practices or help eliminate them. Corporate intent often entails that algorithms are designed to compel consumers towards particular products to drive profits; consumer data allows corporations to "uncover hidden possibilities" and "create highly interactive relationships with [their] customers" (Paley, 2017, p. 4). Moreover, organizational leadership develops strategies for technological implementation, making corporate leadership an input in determining how technologies are designed and applied in an attempt to develop competitive advantages (Paley, 2017). Algorithmic implementation, when used in a corporate context, stems from corporate leadership and reflects their intentions, values, and goals.

Consequences of corporate algorithmic design include the collection, sharing, and selling of user data, while algorithmic outputs profile consumers and market to them specifically to influence their consumptive behaviour. Although I will not discuss in-depth the relationship between corporate intent and its effect on algorithmic design to create outcomes that threaten human autonomy and privacy, it is important to recognize that such threats stem from corporate algorithmic design rather than from the technology itself. To answer research question one (*Can government legislation mitigate threats posed by corporate algorithm use?*) based on the current conceptualizations of algorithms and data in a consumer context, government legislation can restrict corporate algorithmic designs to shape their functional capabilities and influential outputs. As user data is also a key input in shaping algorithmic functions, regulating practices surrounding data collection and processing can shape the way individuals are affected through their interaction with algorithmic outputs. This relationship between algorithmic inputs and outputs also begins to answer research question 3(a) (*How does regulating data-collection and processing shape algorithmic functions to mitigate algorithmic threats to user privacy and autonomy?*), as regulating the way user data is collected and processed may shape algorithmic designs in ways that diminish algorithmic threats.

With regards to research question two (*Can practices of transparency and accountability mitigate threats to user privacy and autonomy?*), it is critical that conceptualizations of algorithmic threats to privacy and autonomy are established in specific context with algorithms operating in a consumer society. In order to understand how government legislation can shape algorithmic technology and alleviate such threats, key concepts such as transparency, accountability, and algorithmic governance must all be clearly understood in specific relation to how they affect algorithmic design and functionality. As the objectives of algorithmic outputs

pose threats to society, mutual shaping theory can inform a preliminary understanding of the relationship between algorithms and consumer society: algorithmic functions, which can shape consumer behaviour and limit their privacy, also foster responses that call for regulations to constrain data-collection and algorithmic functions, which then shape algorithmic functions to limit or enhance the threats they pose to user autonomy and privacy.

Algorithmic Threats: An Overview

There is a growing consensus among scholars that unregulated algorithm use poses threats to society (Flyverbom, Deibert, & Matten, 2017; West, 2017; Foer, 2017; Saurwein, Just, & Latzer, 2017). Algorithms exploit users through data collection and operationalization, and scholars have asserted that three of the most influential information technology and social media companies – Facebook, Google, and Twitter – use algorithms to control the digital content that users access, allowing them to shape public knowledge and consumption patterns (Flyverbom et al., 2017). Additionally, scholars have also identified threats stemming from "data capitalism," an online advertising model where companies use algorithms to target a specific market of users based on their "individual behavioral profiles tied to user data" (West, 2017, p. 4). In data capitalism, corporations gather users' online data, which is then commodified and operationalized via algorithms that shape consumer behaviour (West, 2017). The threat of data capitalism is that it "results in a distribution of power that is asymmetrical and weighted toward the actors who have access and the capability to make sense of data" (West, 2017, p. 4). As companies gather and manipulate user data to influence consumer purchasing trends and drive profits, economic disparity between both parties are furthered (West, 2017). In the process of exploitation, users function as a type of producer as their online actions that provide companies

with data resources (Flyverbom et al., 2017). West's notion of data-capitalism accurately outlines the relationship between user data, their consumptive behaviour, and corporate algorithmic design: corporations gather and utilize user data to determine user consumption patterns and design algorithms to take advantage of such patterns to achieve their financial goals.

Taking a close look at the case of Google, Mager (2012) provides insight into the corporate use of algorithms to influence users' online decision making. Mager (2012) draws on Elmer's (2004) notion of "consumer profiling" to distinguish how search engines gather user data to measure the "desires and intentions of individuals and groups of users," which are then "turned into value through selling them to advertising clients" (p. 772). This "capital accumulation cycle" used by Google exemplifies West's notion of data capitalism as users' search activity is profiled, commodified, and used to influence their behaviour (Mager, 2012). Applying mutual shaping theory to notions of data-capitalism illustrates how the technological advancement of algorithms and data-collection practices occurs as response to socio-economic forces. The rise of data as a valuable resource in consumer marketing has rendered algorithms as a valuable tool for corporations seeking to market efficiently and maximize profits. As socio-economic forces spur algorithmic advancement, subsequent threats to user privacy and autonomy elicit social responses, which shape algorithmic capabilities in turn. Just as economic systems facilitate algorithmic and social change, legal systems will later be viewed to influence algorithmic functions and social responses.

Doneda and Almeida (2016) argue that despite the utility and "valuable output" of efficient instructional processes, algorithms minimize the role of human decision making in online processes. As algorithmic utility grows, they are perceived as increasingly autonomous, challenging human autonomy by influencing our rational processes of decision making (Doneda

& Almedia, 2016). Similarly, Foer (2017) asserts that the corporate shift to data gathering and algorithm use is evidence of an "engineering mind-set" that "views humans as data" in an effort to "make human beings predictable—to anticipate their behaviour, which makes them easier to manipulate" (p. 77). Foer highlights the exploitative power of algorithms which threatens human autonomy and deepens social inequalities.

According to Foer (2017), algorithms express the fallibility and motivations of their human creators, and their outputs are influenced by the inputs gained from human activity. Although algorithms are often perceived as objective, scientific, and impersonal, they are in fact opinionated, rooted in human choices, and subjectively flawed by their creators and input mechanisms (Foer, 2017). The subjective nature of algorithms entails the amplification of bias and discrimination online, especially in cases where algorithms interact with hundreds of millions of users (Foer, 2017). In discussing Facebook's claim that their algorithms are capable of boosting voter turnout and organ donation, Foer (2017) identifies the unnerving power corporations have in influencing individual behaviour through algorithmic outputs.

To expand upon the potential threats posed by algorithms, Saurwein et al. identify a list of nine threats: 1) "manipulation"; 2) "echo chambers"; 3) "constraints on the freedom of communication and expression"; 4) surveillance and privacy threats; 5) "social discrimination"; 6) "violation of intellectual property rights"; 7) "abuse of market powers"; 8) "effects on cognitive capabilities"; 9) "growing heteronomy and loss of human sovereignty and controllability of technology" (Saurwein et al., 2015). There is consensus among scholars that the outlined threats are legitimate, although there seems to be more emphasis on manipulation, surveillance and privacy threats, and social discrimination as the predominant threats across most of the literature. By identifying practices of data collection and user tracking, West's (2017)

notion of data capitalism aligns with Saurwein, Just, and Latzer's (2015) noted threats to user privacy and corporate abuse of market powers. Foer's (2017) understanding of algorithms as online extensions of human bias and discrimination aligns with the threat of social discrimination. As well, algorithms provide individuals with recommendation systems to shape user's online behaviour when they shop online, surf the web, watch videos, and read news (Saurwein et al., 2015). Saurwein et al.'s analysis of recommendation systems outlines the threat of manipulation, which is consistently recognized in the literature on algorithms and internet governance. For my purposes, the threat of manipulation and privacy threats are central to my examination of how government regulation can limit such threats by enforcing practices of accountability and transparency through legislation.

The literature also identifies that algorithms pose threats to users beyond privacy and autonomy; algorithms are capable of furthering social and economic inequality, along with exacerbating bias and discrimination. Such threats may also be limited through practices of accountability and transparency; practices promoting corporate accountability towards users may shape key algorithmic inputs by regulating practices of data-collection and processing. Examining whether or not practices of accountability and transparency may lessen algorithmic threats that further inequality, bias, and discrimination requires a critical analysis of these threats separately, with conceptualizations drawn in specific context with consumer society. However, this paper will remain focused on how practices of accountability and transparency can specifically mitigate algorithmic threats to individual autonomy and privacy. To understand the relationship by which practices of accountability and transparency can diminish threats to individual autonomy and privacy, each key concept must be examined in specific context with algorithmic functions.

Threats to User Autonomy

Algorithms are often applied in digital marketing to shape individual behaviour and influence the consumption of goods and services (Just & Latzer, 2017). In addressing such threats to human autonomy, Gal and Elkin-Koren (2017) assert that algorithms are often designed to fulfill corporate interests rather than the best interests of consumers. Since algorithmic functions can be manipulated through their inputs, and since algorithms are often technically complex and difficult to "understand, decipher, and challenge", it becomes more difficult for consumers to protect themselves from an algorithm's manipulative power (Gal & Elkin-Koren, 2017, p. 324). These algorithms create "feedback loops" of consumer content that are "designed to narrowly calibrate human desire and activity towards market- and financial-friendly equilibrium" (McKelvey, Tiessen, & Simcoe, 2015, p. 579). For corporate parties, algorithmic functions are a product for their own profit-driven interests, and algorithms are designed to create outputs – that is, content or product suggestions – that manipulate consumer behaviour. In essence, algorithmic capacity for consumer manipulation is possible as human judgement is replaced by non-transparent code (Gal & Elkin-Koren, 2017). Like Foer (2017), Gal & Elkin-Koren (2017) also noted how Facebook's algorithms have proven capable of affecting user emotions as they use the platform. However, it is important to recall that issues of algorithmic manipulation are a result of algorithmic design. A lack of user understanding of algorithmic functions and design entails a lack of understanding of how algorithms affect them by collecting their data and processing it to later influence their decision-making as consumers. This notion is important for further discussion on algorithmic transparency, especially as transparent practices among corporations may affect the way users understand algorithmic function and design, which may then shape the way users are influenced.

Digital intermediaries design algorithmic applications for corporate actors seeking to utilize algorithms to achieve their goals. As digital intermediaries operate as a separate party between consumers and corporations, they may be less accountable to users despite the role they play in designing algorithmic applications for corporations. The role of digital intermediaries outlines how corporate design of algorithms can limit user autonomy by creating algorithmic functions designed to manipulate consumer behaviour for corporate benefit. Van Loo (2017) studies some of the effects that "digital intermediaries" have on consumers, especially with regards to how they "influence people's decisions in transacting with private entities" (p. 1280). According to Van Loo (2017), digital intermediaries are tools that provide algorithmic advice and are distinct from private sellers of a product or service. As digital intermediaries essentially sell use of their algorithms, they are complex, multidimensional, and are capable of influencing consumer perception as they shop online (Van Loo, 2017). By leveraging vast databases of consumer information to determine trends and behaviour, algorithms provided by digital intermediaries are capable of "[nudging] consumers to higher-margin products" (Van Loo, 2017, p. 1277). Van Loo goes on:

> Overall, private digital intermediaries can fall short of expectations. They may lack the information they need to enhance decisionmaking. Even if they have the necessary information, they can add a new layer of exploitation by inserting shrouded fees or raising prices. Although one perceived benefit of intermediaries is the avoidance of choice-limiting governmental regulation, digital intermediaries may restrain seller autonomy. (Van Loo, 2017, p. 1296)

As digital intermediaries operate between consumers and corporations, algorithms operationalize consumer data in order to manipulate their consumption to the benefit of corporations, which in

turn pay for the algorithmic services of the intermediary responsible for the design of the algorithms. In this process, there is no accountability to the public by intermediaries that design such algorithms for corporate use. Restricting the way digital intermediaries can collect user data, operationalize it, and share with other corporate actors can mitigate corporate manipulation of consumer behaviour by limiting the inputs required to develop behavioural profiles and market trends.

Threats to User Privacy

Information and communication technologies, including algorithms, are "neutral" in terms of posing privacy threats; whether a technology enhances or invades an individual's privacy is dependent on the technological design (Cavoukian, 2009). In conceptualizing privacy in context with algorithms, it must be emphasized that algorithms are capable of enhancing privacy for users, rather than exclusively threatening it. For Cavoukian (2009), privacy-enhancing technologies "embody fundamental privacy principles by minimizing personal data use, maximizing data security, and empowering individuals" (p. 5). Once again, algorithms do not inherently pose privacy threats to individuals, yet they are often designed to function based on the mass-collection and processing of user data, with the intention of using such data to market to consumers in ways that influence their consumer decision-making.

One of the key ways algorithms impact society is the manner in which they are designed for the mass collection of user data, which threatens the privacy of Internet users. In relation to mobile banking applications and the vast amounts of user data collected to provide banks and users with advanced analytics, Sreejesh, Anusree, and Amarnath (2016) argue that "clandestine collection of personal information is seen as intrusive and a violation of users' privacy" (p.

1098). Further threats come as a result of modern cloud computing environments where data is stored in online networks or "virtual environments" that are "targets for privacy breaches" (Adams, 2017). Although algorithmic functions do not inherently pose threats to user privacy, the mass collection of user data poses threats to user privacy. These vast databases of user information are a constant target for cyber criminals who seek to exploit them for personal gain. In fact, legislative act 85 of the GDPR's regulations highlights a number of privacy threats that can arise as a result of a data breach:

> A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. (General Data Protection Regulation, 2018, L 119/16)

Since databases of user information are valuable targets, threats to user privacy arise in cases where vast amounts of user data are collected for corporate use. Yet one cannot assume that corporations with vast databases of user information will remain accountable to users in cases where their privacy is breached. In September 2017, Equifax announced that a data security breach had been discovered in July 2017, which affected approximately 143 Americans (Equifax, 2017). While this data breach prompted investigations from state attorneys and U.S. Congress, there was no legislation in place to enforce standardized penalties, and the breach only subsequently prompted the proposal of the U.S. "Data Breach and Compensation Act", which would have imposed mandatory fines on Equifax had it been in effect (Henning, 2017;

Puzzanghera, 2018). By establishing practices of accountability and transparency through government legislation, corporations may be forced to take further measures to inform and protect users from privacy threats stemming from compromises of data-security. Government legislation may be able to regulate corporate algorithmic design to align more closely with Cavoukian's (2009) understanding of privacy-enhancing technologies.

Overall, my literature review suggests thus far that algorithmic threats to user privacy stem from the mass collection of user data, while threats to user autonomy stem from the processing or operationalization of data to create marketing strategies that influence consumer decision-making. Each data security threat involves how users are affected by practices of data collection and processing, and government legislation has the capacity to regulate the scope by which corporates can collect and process user data. To answer research question one, government legislation has the capacity to weaken algorithmic privacy threats by regulating corporate data-collection practices, as well as how they store and secure user data.

Yet this insight gleaned from the literature in response to research question one begs the question as to how algorithms can be regulated to change the way they interact with individuals to mitigate threats. This is the issue highlighted by research question two, which seeks to understand how practices of transparency and accountability serve to mitigate threats to user privacy and autonomy by regulating algorithmic interactions with users. As legislation affects data-collection practices that serve as algorithmic inputs and threaten user privacy, regulatory practices of accountability and transparency can shape algorithmic design to function in ways that are less invasive to user privacy. By regulating practices of data-collection and processing, algorithms may not only pose decreased privacy threats but also decrease user manipulation by restricting inputs so that algorithmic functions are limited to a specific mandate. In other words,

addressing privacy threats by regulating data-collection and processing may indirectly affect algorithms' influential capabilities. With regards to Van Loo's (2017) notion of digital intermediaries, for example, legislating the processes by which digital intermediaries collect and share data can also protect user privacy by limiting the free-flow of user data between parties. Nevertheless, conceptualizing practices of transparency and accountability in context with algorithms that operate in a consumer society will assist in identifying how they may promote user autonomy and privacy.

Governance, Transparency, and Accountability

Internet Governance

While the threats algorithms pose to society identify the influence they have in shaping individual behaviour and society, there is a capacity for governments and corporate authorities to influence the usage of algorithms through regulation. Scholars suggest that algorithmic regulation can be self-imposed by corporations, or established through government legislation (Doneda & Almeida, 2016; Gasser & Almeida, 2017). In either case, regulatory measures can encourage practices of accountability and transparency to mitigate algorithmic threats (Mager, 2012; Doneda & Almeida, 2016; Gasser & Almeida, 2017; Just & Latzer, 2017). Although this paper only explores how government legislation can mitigate algorithmic threats by enforcing practices of transparency and accountability among corporations, organizations that design and utilize algorithms are capable of self-regulation.

Despite the potential effects internet governance can have on algorithm use, scholars have identified several factors that contribute to a governance gap in algorithmic usage and regulation. First, cases of algorithmic governance by a state exist on an relatively minimal scale internationally in comparison to cases of algorithm governance by private actors (Just & Latzer,

2017). Second, when compared to governments and other influential parties, corporate actors disproportionately utilize algorithms to govern individual behaviour (Just & Latzer, 2017). Third, with minimal government regulation and the potential to manipulate user behaviour and consumer patterns, corporate algorithm use has become increasingly opaque and unaccountable at the expense of user agency (Just & Latzer, 2017).

Doneda & Almeida (2016) suggest that an industry-wide set of standards and practices ought to be established to regulate algorithm use, while a "governmental oversight body in charge of algorithm regulation" can focus on limiting threats and maintaining security in user data collection (p. 62). They also suggest that regulation can begin by legislating the data-collection practices upon which algorithms depend (Doneda & Almedia, 2016). Although there are particular instances of regulation to lessen algorithmic threats, the role of states in algorithm governance is internationally ambiguous due to uncertainties about how algorithmic technologies and markets will develop (Saurwein et al., 2015). Furthermore, internet governance "is characterised by the absence of a coherent regime or organisation in charge of enacting globally consistent and comprehensive norms and policies," which limits the existence of "accountability structures" (Eggenschwiler, 2017, p. 5). While there are instances of corporate efforts to establish ethics boards and quality control protocols, companies are diverse and incongruent in their purpose and are in competition with each other, which has so far prevented the development of universal standards for corporate algorithmic regulation (Saurwein et al., 2015). Nevertheless, there remains a need for government intervention as corporations continue to limit transparency in order to prevent algorithmic manipulation and imitation (Saurwein et al., 2015).

Similar to how social forces and technology influence each other according to mutual shaping theory, algorithmic governance can be characterized as a medium for socio-

technological change. As societal influences respond to algorithmic threats, government legislation serves as a legal facilitator of technological change. Algorithmic governance therefore exists at an intersection of social and technological forces that influence each other in a co-evolutionary process; algorithmic legislation serves as a mediator in responding to both algorithmic threats and societal reactions, and has the potential to shape technological limitations as well as social perspectives. While algorithmic governance can serve as a facilitator for both social and technological change, certain practices of transparency and accountability can mitigate algorithmic threats when applied to legislation.

Transparency and Accountability

As the aforementioned scholars identify the threats algorithms pose to society, others go further in identifying how principles of accountability and transparency can assist in establishing regulatory practices to limit such threats. In regard to algorithmic threats, scholars note that the highly technical nature of algorithms can undermine transparency, while accountability is required to draw attention to the parties liable for their usage and ensure responsible and fair use of algorithms (Doneda & Almedia, 2016). Doneda and Almedia note that practices of accountability and transparency are not yet applied robustly in algorithmic regulation despite their potential to mitigate algorithmic threats (Doneda & Almedia, 2016). To allow for transparency and accountability, Internet governance could focus on increasing user privacy and limiting the user-exploitation machine that commodifies user activity (Mager, 2012). To adequately identify how principles of transparency and accountability can be applied in practice to diminish algorithmic threats, each concept must be explored in relation with algorithmic governance and consumer society.

Transparency

Notions of transparency in the context of governance are often vague. In spheres of democratic global governance, transparency may often be considered as a 'buzzword' or jargon (Hale, 2008). Transparency needs to be conceptualized in the specific context of algorithmic governance to understand the role that transparent practices have in mitigating algorithmic threats. Weber (2008) notes that transparency is both a regulatory attribute and goal that encompasses "clarity, accountability, accuracy, accessibility, and truthfulness" (p. 344). There are three types of transparency in Internet governance: procedural, decision-making, and substantive (Weber, 2008). Procedural transparency entails that organizations follow rules and procedures to foster clarity, unambiguity, and public disclosure, while also allowing for the public to access and understand processes of governance and lawmaking (Weber, 2008). Decision-making transparency focuses on public access to political mechanisms and government decisions. Finally, substantive transparency focuses on rules and standards to prevent arbitrary and discriminatory decisions (Weber, 2008). Conceptualizing transparency with a focus on Weber's procedural type is most suitable in specifying the role transparent practices have in mitigating algorithmic threats. Weber's typology of transparency is preferable to my analysis as characteristics of clarity, unambiguity, and public disclosure serve as key principles that promote user awareness when put into practice in relation with algorithmic governance. Procedural transparency is relevant in this context because it emphasizes the relationship between rules for transparency and their effects on organizational practices and outcomes. For the purpose of this MRP, practices of transparency ought to be understood as rules and procedures established to foster public understanding and scrutiny of processes of data-collection and operationalization that serve as algorithmic inputs and outputs respectively. Practices of transparency can be

observed in government legislation, which aims to encourage public understanding of how corporations collect and operationalize user data through algorithms to influence consumer behaviour, and in the way such legislation specifically reduces threats to user autonomy and privacy.

When deployed effectively, transparent practices enable powerful institutions and individuals to be held to account. Mayer-Schonberger and Lazer (2007) note that, "without transparency, there is no accountability and citizens cannot make informed decision about democratic delegation of power" (Mayer-Schonberger and Lazer, 2007, p. 285). In principle, this notion can be extended to the interactions between corporations and individuals. Although transparent principles are not justified among private actors, the relationship between corporations that utilize algorithms and the individuals that are affected by them entails significant corporate control of such individuals' behaviour and private information. Without transparency, individuals are less capable of making informed decisions about how corporations ought to utilize algorithms to affect consumer society. With greater transparency around the design, purpose, and functions of algorithms, users are capable of making more independent decisions about which products or services to purchase online.

In relation to algorithmic technologies specifically, Foer (2017) highlights the relationship between algorithms and a lack of transparency through the example of Google. He notes that Google founders Larry Page and Sergey Brin initially opposed the notion of advertising-funded search engines because advertising-driven incentives compel the design of algorithmic technology to pursue profit over transparency. He quotes them saying, "we believe the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm" (Foer, 2017, p. 212). Since 2012,

Google has implemented advertising into their search engine as they shift towards a more profit driven business model. Now, advertised pages appear before other search results, and while they are labelled as "ads", Google's algorithm privileges the pages of advertised parties, nudging users towards their products and services over others. Such an example illustrates how algorithmic design, when mixed with profit-driven incentives, decreases transparency for users as they use algorithmic services.

Similarly, corporations seek to limit algorithmic transparency by treating algorithmic design as a "trade secret" (Vedder & Naudts, 2017). As algorithmic functions can serve as a competitive advantage for corporations when marketing to consumers, maintaining the secrecy of its design is rational from a corporate perspective. Consequently, algorithmic design is inclined be opaque, both for consumers who are affected by algorithms, as well as for corporations in competition with each other. Among corporations, the technical designs – or "source code" – of algorithms often remain opaque due to their proprietary nature, but this source code would likely be unintelligible to the average consumer if they had access to it anyway (Vedder & Naudts, 2017). Algorithmic transparency, therefore, should not necessarily focus on providing the common user access to the technical code of algorithms, but rather provide clear information as to how algorithms operationalize their data for specific purposes, while also explaining how such data is collected and shared. The problem with opacity in this non-technical context is that it becomes increasingly difficult for users "to assess whether or not algorithmic decision-making is desirable in a given situation" (Vedder & Naudts, 2017, p. 210). Overall, the lack of non-technical algorithmic transparency likely stems from the corporate intention to influence consumer behaviour through advertising and direct-marketing. The role of user awareness is important in discussing transparency and algorithmic threats to autonomy in

particular. With transparent understanding of data-collection practices and algorithmic functions, increased user awareness may serve to mitigate an algorithm's capability to influence consumer behaviour.

Accountability

Accountability can also be a vague concept and it must be conceptualized in relation to algorithmic regulation to understand how accountable practices can mitigate algorithmic threats. In simple terms, practices of accountability can be identified based on two characteristics: "the ability to know what an actor is doing and the ability to make that actor do something else" (Hale, 2008, p. 74). Weber (2011) defines accountability broadly as an obligation of one party to another where the accountable party must explain and justify all actions affecting the party subject to their influence, while also taking responsibility for harm caused by one party to another. In the context of Internet governance, effective methods of accountability include three elements: organizational standards to hold governing bodies accountable, an active flow of information so affected parties can hold accountable parties responsible to the agreed upon standards, and sanction procedures to discipline accountable parties when they fail to meet those standards (Weber, 2011). This framework serves as a specific way of evaluating the degree to which practices of accountability are present in Internet governance. Practices of accountability can be evaluated according to this framework to determine if they are a theoretically effective means of mitigating algorithmic threats to human autonomy and privacy.

As a principle, accountability is commonly associated with democratic institutions, which may provide insight as to how accountable practices may diminish algorithmic threats. For instance, bureaucratic structures are comprised by accountability, budgeting, legislation, and

agency autonomy (Fountain, 2007). Fountain's (2007) emphasis on the bureaucratic structure demonstrates how accountability stems from a hierarchy where those in superior positions are held accountable to those beneath them. In relation to corporate actors, algorithmic functions, and the individuals subjected to them, there is no sanctioned structure that elicits corporate accountability to users. Bureaucratic structures and mechanisms of accountability exist within corporate organizations, and many corporations are held accountable to individuals for their products or services through contracts and terms of service. However, systems of accountability are limited for users who interact with corporate actors online as they utilize their free services and are subjected to direct-marketing. A lack of accountability becomes apparent when personal data is collected and users lack control over information collected from them. Legislation may function to create mechanisms of accountability between corporations and users, thereby extending the bureaucratic structure that exists within organizations to include users, who serve as 'prosumers' in many cases by generating the data that corporations use and sell, and who interact with organizations despite existing outside of the formal corporate structure.

Control and oversight mechanisms may further practices of accountability to regulate corporate data-collection and algorithm use in ways that mitigate threats. In relation to democratic government accountability, Coglianese (2007) notes that bureaucratic delegation weakens government accountability to citizens, yet requiring that elected legislators solely determine the regulatory agenda is impractical and inefficient. However, Coglianese (2007) notes that the solution to this issue is institutional control and oversight. Control depends on statutes which define the specific authority and a scope of operation for government agencies, while oversight entails that "legislators hold hearings at which they summon the leaders of regulatory agencies to produce information and answer questions" (Coglianese 2007, p. 109).

Through institutional control and oversight, the legislature remains accountable for the actions and decisions of the bureaucratic delegates, which then translates to accountability towards constituents.

While the foregoing discussion applies specifically to governments, notions of indirect accountability through control and oversight can be applied in other institutional contexts. In cases where digital intermediaries are involved, for example, corporations are capable of overseeing the function of an algorithm for their purposes. For corporations that develop their own algorithms, they possess full control over their data-collection practices and design of algorithmic functions to achieve desired outputs. Corporations utilizing algorithms are capable of implementing control and oversight mechanisms to further accountability to users, yet a lack of corporate accountability has been identified. However, government legislation is capable of implementing practices of accountability by requiring that corporations establish mechanisms of control and oversight according to a set of standards.

The Relationship Between Accountability and Transparency

Based on scholarly conceptions of accountability, practices of transparency help bolster practices of accountability. Hale (2008) identifies the first characteristic of accountability to be "answerability", or "the ability to know what an actor is doing" (p. 74). As practices of transparency establish open channels of communication between parties, they also help fulfill the "answerability" element of accountability. Therefore, practices of accountability and transparency are intertwined to an extent; institutionalized channels that convey information between parties are prerequisites for both practices of accountability and transparency. In relation to algorithmic governance, the creation of active information flows begins to fulfill

characteristics of both accountable and transparent practices. Yet practices of accountability constitute more than active information flows, they include organizational standards, institutionalized penalties, and mechanisms of control and oversight. To answer research question two, practices of accountability can mitigate threats to user privacy by: standardizing internal mechanisms of control and oversight among organizations to protect user data and privacy, institutionalizing information flows regarding data collection and processing between users and organizations, and imposing penalties for regulatory violation. Furthermore, practices of transparency can mitigate threats to user autonomy by using the same information channels to promote user awareness of data-collection practices and algorithmic functions, allowing users to make informed decisions as to how to protect their privacy and object to influential marketing tactics.

Practices of accountability may be more effective at mitigating threats to user privacy, while practices of transparency may be more effective at mitigating threats to user autonomy. As corporate actors lack mechanisms that evaluate the security of user data, and do not possess the appropriate channels to provide users with relevant information regarding how their data is collected, shared, processed, or even stolen, data collection poses threats to privacy through a lack of accountability to users. Furthermore, data-collection and operationalization pose threats to autonomy through a lack of transparency and user awareness, primarily because a lack of awareness furthers minimal understanding of how data is operationalized, thereby limiting the decision-making capacity of users when exposed to influential marketing tactics. Consequently, practices of accountability primarily limit threats to user privacy as they create mechanisms to control and oversee corporate collection and processing of data, while also establishing communication protocols between each party. On the other hand, transparent practices may

primarily limit threats to human autonomy by creating user-awareness (of corporate practices of data collection and processing) through the same communication channels to promote informed decision-making among users. Nevertheless, practices of transparency support practices of accountability (Hale, 2008), especially as both practices rely on effective communication channels between parties. As a result, the two practices applied together are capable of mitigating algorithmic threats to user privacy and autonomy.

Theoretical Approach

Developing democratic governance solutions to combat algorithmic threats requires that connections be drawn between modes of regulation, the contexts of regulation, and theories of technology and society. Before analyzing the GDPR, an adequate theory regarding the relationship between technology and society must be explored to frame the analysis and discussion. Technological determinism does not serve as appropriate framework for analyzing the relationship between internet governance and algorithmic threats because it understands technology as the primary determinant of societal outcomes. According to theories of technological determinism, technologies transfer their characteristics to users in ways that shape their identities, "imprinting themselves on users' individual and collective psyches" (Baym, 2015, p. 29). Yet internet governance, practices of data collection, and technological design all serve as inputs that shape the function of algorithms. At the other end of the spectrum, social constructivism is also inadequate as it focuses, for the most part, on societal effects that shape technology. For social constructivists, "social forces influence the invention of new technologies" as creators of technologies are embedded in social contexts that render the technology dependent on societal forces (Baym, 2015, p. 45). Legislation such as the GDPR may be understood as a form of social constructivism that seeks to restrict algorithmic threats in

response to technological deterministic anxieties. Such a perspective appropriately identifies the significant role that society and legislation have in shaping the application and effects of algorithmic technologies. In fact, legislation like the GDPR may theoretically empower social forces to the extent that they are more dominant in shaping algorithmic technologies than vice versa. However, considering the theoretical efficacy of the GDPR and its practices of accountability and transparency should not neglect the role technology plays in influencing society, especially as algorithmic effects may induce the technological deterministic anxieties that influence the policy agenda. Mutual shaping theory therefore assists in analyzing how such practices may mitigate algorithmic threats through legislation, primarily because legislation empowers social forces in shaping technology despite technology's apparent effects on society.

In his discussion of mutual shaping theory, Boczkowski (1999) notes that technological artifacts such as algorithms are not exclusively "constructed by their designers" but also "reconstructed by their users" (p. 91). Technological artifacts like algorithms both "enable and constrain certain types of social action, and users may either leave those features untouched or attempt to modify them" (p. 91). Boczkowski emphasizes that there is a mutually constituted process of enabling and constraining technological and social change. In this process, Boczkowski argues, technological change triggers the mediation process for social change, and social change recursively triggers the mediation process for technological change. Applied to algorithm use and internet governance, a mutual shaping framework is most appropriate for analyzing correlations between regulation, accountability, transparency, and the threats outlined in the literature.

A basic relationship between government institutions and corporate organizations illustrates how the mutual shaping theory frames the relationship between algorithmic threats and

governance. According to Fountain (2007) government institutions use laws and regulations to "constrain organizations that, in turn, shape individual and group behaviour in social networks" (Fountain, 2007, p. 75). In the case of the GDPR, government legislation is used to constrain organizations' practices surrounding data-collection and processing. As well, the GDPR requires that organizations adhere to new procedures to protect user information, remain accountable in its use and protection, and remain transparent by providing requested information. As the GDPR shapes the actions of corporations that design and utilize algorithms, the function of algorithmic technologies are shaped by the legislation. On the other hand, algorithmic technology and mass data-collection shaped the GDPR to begin with, because the GDPR came as a response to a regulatory gap surrounding new technological capabilities. Considering how user data serves as a key input in producing algorithmic outputs, the GDPR significantly shapes the capabilities of algorithmic technology by regulating data-collection. On the other hand, the threats to user autonomy and privacy highlight the capacity of algorithms to shape society by influencing individuals in a consumer context. To go even further, algorithmic design is shaped by society because of its reliance on user data as an input that shapes its functions. Although I have only explored algorithmic technologies in a consumer context, it is reasonable to presume that algorithmic technologies are capable of influencing society in other contexts as well. In employment, for example, algorithmic biases may influence hiring processes, influencing managers' hiring decisions despite attempts to remain "neutral" and objective (Mann & O'Neil, 2016).

To extrapolate based on mutual shaping theory, algorithmic technologies and legislations targeting them are mutually constituted. While there are many ways that algorithmic technology

shapes society and vice versa, I will specifically explore the mutually constituted relationship between government legislation and algorithmic functions by using the GDPR as a case study.

The European Union General Data Protection Regulation

> *Personal data is the gold of the 21st century. And we leave our data basically at every step we take, especially in the digital world. The Facebook/ Cambridge Analytica scandal showed this very clearly and confirmed that we are doing the right thing in Europe. The scandal reminded us that these rules go beyond data protection and are also important to protect our democracy and free elections.*
>
> -Věra Jourová, EU Justice Commissioner (European Commission, 2018)

The EU *General Data Protection Regulation* (GDPR) was initially proposed in 2012, approved in April 2016, and enforced as of May 25th, 2018 (GDPR Timeline of Events, 2018). The GDPR is meant to update and replace the EU's *Data Protection Directive* (1995/46/EC) (Bhaimia, 2018). According to European Data Protection Supervisor, Giovanni Buttarelli (2016), the GDPR will be facilitated by the European Data Protection Board "to foster that trust and accountability, by being transparent and accessible to stakeholders" (p. 77). The GDPR incorporates principles of transparency and accountability by implementing data subject rights – or user rights – that include rights to transparent information, "conditions for consent", "right of access", "right to be forgotten", and the "right to object" (Summary of Articles Contained in the GDPR, 2018). This is corroborated by Vedder and Naudts (2017) who state that accountability and transparency are "becoming even more important as guiding protection principles in the upcoming European General Data Protection Regulation" (p. 211). Since data is an input that algorithms require to function, regulating the way data controllers – or corporate actors – collect and process data can shape algorithmic functions and potentially mitigate the threats they pose to

society. The reliance of many algorithms on the collection of personal data entails that algorithmic functions are within the scope of the GDPR (Vedder & Naudts, 2017).

Territorial & Governmental Scope

The case of the GDPR is an example of data regulation that is mobilized through multi-lateral government legislation. Article 3(1) and 3(2) state that the territorial scope of the EU GDPR applies to organizations that process or control an individual's personal data who resides in the EU even if such processing does not geographically occur in the EU itself (General Data Protection Regulation, 2018). The territorial scope therefore protects all individuals residing in the European Union, rather than regulating data controllers that operate specifically within the EU. As a result, the GDPR is capable of influencing practices of data collection and processing internationally, but only in circumstances where an organization is interacting with a resident of a EU member state. Because the EU is a multi-lateral political and governmental union, the scope of their legislative authority is larger than a typical government (Buttarelli, 2017). The territorial and governmental context of the EU is significant in assessing the potential efficacy of the GDPR as it is a societal factor that contributes to shaping of algorithmic technologies. Given the GDPR's governmental and territorial contexts, it may also have a greater capacity at shaping data collection and processing for individuals that reside outside of EU member states as well. Each of these aspects will be explored further in the discussion section while also considering the mutual shaping theory.

Transparency Through Awareness: Rights to Access and Clear Terms

The GDPR establishes practices of transparency and accountability by institutionalizing the "right to access", which establishes standardized channels for active information flows between users and organizations that collect and process their data. Whereas the previous Directive allowed organizations to provide extensive, legally complex, and ambiguous terms of agreement for collecting and processing user data, the GDPR requires organizations to offer terms that are straightforward and concise (Bhaimia, 2018). Article 12 of the regulation, "transparent information, communication and modalities for exercising the rights of the data subject", outlines how organizations must provide information to data subjects in a transparent fashion to communicate how their data is controlled and processed (General Data Protection Regulation, 2018, p. 39). Data subjects have rights to receive all information related to their personal data as outlined in the GDPR (articles 15-22, and 34 of the regulation) and communications and consent forms sent by data controllers must be written "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" (General Data Protection Regulation, 2018, p. 39).

Article 12 aligns with Weber's notion of procedural transparency as it promotes clear and unambiguous information flows so users can understand how their data is controlled and processed. Therefore, article 12 enforces transparent practices among organizations that collect and control user data. Allowing users to request such information from data controllers may also allow for increased user awareness regarding the collection and operationalization of their data. In turn, this practice of transparency has the potential to mitigate threats to user autonomy in a consumer context; as data subject rights make users aware of how their data is collected and

stored, they can knowledgeably decide to object to data collection and processing if given the opportunity, or avoid these online interactions altogether.

In exploring how such data subject rights allow for transparency, Malgieri and Comandé (2017) suggest that user awareness and empowerment can be broken down into three tiers: readability, explanation, and legibility (p. 245). "Readability" fosters understanding of data, also enhancing comprehensibility of data based algorithms, yet it does not "foster transparency automatically" as it neglects the scope, purpose, and implications of such algorithms (Malgieri & Comandé, 2017, p. 245). "Explanation" entails retroactively providing information regarding "data processing and decisions taken about a specific customer/user" (Malgieri & Comandé, 2017, p. 245). "Legibility" entails the combination of the "comprehensibility of the functioning of the algorithm […] with transparency about the commercial use of that algorithm" (Malgieri & Comandé, 2017, p. 245). Algorithmic transparency increases for users as they receive explanation about how their data is used and legibility regarding the purpose their data serves in creating algorithmic outputs. With reference to the GDPR, Malgieri and Comandé find that the emphasis on data subjects receiving "meaningful information about the logic" of algorithmic processes ensures transparency and comprehensibility for users receiving information (Malgieri & Comandé, 2017, p. 257). The mere "knowledge" of detailed information surrounding algorithmic processes ensures transparency but not comprehensibility, yet comprehensibility is present in the GDPR via Article 7, which also highlights clear and straightforward terms for users as they provide their consent (Malgieri & Comandé, 2017, p. 257). In any case, Malgieri and Comandé (2017) discern how the GDPR's active information channels and clear terms seem designed to foster transparency and enhance user awareness through legibility.

In the event that the data controller does not take action to provide users with requested information, Article 12(4) of the regulation also highlights how they must inform the data subject of reasons why they did not respond to the request as well as inform them of the legal action and complaint protocols they can take with supervisory authorities (General Data Protection Regulation, 2018, p. 40). Article 12(4) embodies practices of accountability as it provides standards by which data subjects can hold data controllers accountable for their actions, or lack of actions, while also creating protocols for communication between organizations and users so that both parties can understand if and how standards are being met. Accountability to users is established further as data processors and controllers will face fines of "4% of annual global turnover" – up to a €20 Million maximum – for breaching the user rights and operational standards outlined by the GDPR (GDPR FAQs, 2018). As data controllers are subject to financial penalties for failing to observe the standards outline by the GDPR, all of Weber's criteria for accountable practices are met.

Furthermore, a user's right to access confirms if and how their personal data is being processed in a transparent fashion. Article 15 of the regulation outlines a data subject's right to access detailed information regarding the extent to which their personal data collected, how it is processed, how long it is stored for, which third parties will have access to it, and if it is used for automated decision-making and profiling (General Data Protection Regulation, 2018, p. 43). As data subjects are able to access information regarding their personal data in a straightforward manner, user autonomy may be enhanced as data controllers convey data-processing activities "to the general public in a transparent manner in order for the public to be able to make informed decisions" (Vedder & Naudts, 2017, p. 214). Here, transparency is closely tied to the notion of user awareness of how their personal information is processed. According to Vedder and Naudts

(2017), algorithmic transparency encourages public knowledge in ways that allow users to make informed decisions. As practices of transparency improve user awareness, threats to user autonomy may theoretically decrease as users become aware how algorithms may affect their decision making. Increased awareness of algorithmic purposes and functions enables users to make more informed consumer decisions given their knowledge of algorithmic influence. Provided that users are given the opportunity to opt-out of direct marketing practices, they can also knowledgeably decide whether or not they wish to be influenced by targeted ads generated by algorithms based on their data-profiles. With regards to research question three, data subject rights to access information about algorithms in clear terms embody practices of transparency as they promote user awareness of how their data is collected and processed. As users become aware of how their data may be collected, shared, and processed to influence their consumer behaviour, they can begin to make decisions that bolster their consumer autonomy.

Accountability Through Control: The Right to be Forgotten

Article 17 of the regulation outlines a data subject's "right to be forgotten", which allows users to demand that data controllers and processors erase and cease further dissemination of their data (General Data Protection Regulation, 2018). The right to be forgotten demonstrates how the GDPR implements practices of accountability by establishing control mechanisms that restrict the authority and scope by which data controllers collect and process data. The right to be forgotten outlines a number of circumstances when data subjects can request the erasure of their data. These include but are not limited to the following circumstances: a subject's data is no longer relevant for the original purpose it was collected or processed for; the user withdraws consent to the processing of their data; the user objects to direct-marketing as per their rights

outlined in Article 21; the user's data is "unlawfully processed" or subject to erasure based on "compliance with a legal obligation in Union or Member state law" (General Data Protection Regulation, 2018, p. 43-44). Each of these circumstances that justify erasure of user data sets limits on the way data controllers manage user data. The circumstances in which users can request that their data be deleted each constrain the scope of data that is retained by data controllers. Just as the legislature in a democratically elected government maintains accountability to constituents by providing control mechanisms to regulate the authority of bureaucratic agencies, the GDPR forces data controllers to remain accountable to data subjects through control mechanisms which limit data controllers' authority when managing user data.

Such practices of accountability, established through control mechanisms such as the right to erasure, have the potential to protect user privacy by allowing users to limit the extent to which their data is collected and retained. The right to be forgotten may minimize vast databases of user information, potentially decreasing threats to user privacy by constraining mass accumulation of user data. To begin to answer research question three, regulating the context by which data is retained is an important accountability measure in regulating practices of data processing. Based on my framework of accountability, the GDPR may limit algorithmic threats to privacy through accountable practices of control that restrict data collection and retention within necessary bounds outlined by the user and legislation.

Accountability Through Oversight: Mechanisms of Internal Governance

The GDPR furthers accountability by requiring that organizations demonstrate compliance by creating mechanisms of internal governance (Bhaimia, 2018). Such measures include maintaining an internal record of data processing activities, conducting "Data Protection

Impact Assessments" (DPIA), and appointing a "data protection officer in certain circumstances" (Bhaimia, 2018, p. 25). DPIAs require that data controllers assess the potential risks and consequences of processing personal data in cases where doing so "is likely to result in a high risk to the rights and freedoms of natural persons involved" (Vedder & Naudts, 2017, p. 213). DPIAs identify how government legislation can establish practices of internal corporate self-regulation. DPIAs are significant accountability measures because they exemplify oversight mechanisms. Similar to how democratic legislators maintain accountability by holding oversight hearings for regulatory agencies, the GDPR demands that data controllers remain accountable to users by establishing internal governance structures that oversee the protection of user data in compliance with security standards. By requiring that corporations evaluate the potential risks to user rights and freedoms as they collect their data, accountability to such users can be established if corporations oversee proper compliance with regulations on users' behalf. Although such mechanisms of internal regulation are not self-imposed, the GDPR is likely to force corporate actors to establish internal mechanisms to facilitate accountability towards users.

It was previously noted that, as long as vast databases of user information are produced, privacy threats endure due to the possibility of a data-breach. Legislative act 85 of the regulation outlined some of the privacy threats that data-breaches can pose, and it goes on by declaring that controllers shall notify supervisory authorities of such data-breaches within 72 hours of becoming aware of them (General Data Protection Regulation, 2018, p. 17). To further accountability of data controllers towards data subjects, legislative act 86 of the regulation demands controllers notify subjects of a data-breach affecting them. It goes on:

> The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects.

> Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. (General Data Protection Regulation, 2018, p. 17).

Through act 86, the GDPR standardizes practices so that data controllers are accountable towards data subjects to ensure they are adequately informed of breaches affecting their personal data. Although this act does not outline any actions for compensation or recuperation, it does hold data controllers accountable to subjects by ensuring active information flows to data subjects. To answer research question three, act 86 has the potential to diminish threats to user privacy by creating oversight mechanisms where data controllers must remain accountable to data subjects by following standardized procedures to protect the privacy of subjects when security protocols are breached.

The Right to Object to Direct Marketing

Although the GDPR regulates practices of data collection that serve as algorithmic inputs, regulating data collection may only marginally limit the operationalization processes that create algorithmic outputs. The GDPR's data regulation may not entirely mitigate algorithmic manipulation of users to influence their behavioural processes and decision making. However, article 21 of the GDPR regulation states that:

> Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. (General Data Protection Regulation, 2018, p. 45)

Furthermore, legislative act 70 of the regulation also identifies that the right to object to direct marketing "should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information" (General Data Protection Regulation, 2018, p. 13). The ability to opt-out of direct marketing may limit the capability organizations have in manipulating users' consumptive behaviour. As the ability to opt-out is explicitly brought to the attention of users, it may limit algorithmic influence and increase awareness of how user data is operationalized. The ability to object to direct marketing empowers data subjects to act upon practices of transparency that enable user awareness outlined in their rights to access and clear terms. This awareness may shift users' understanding of how their online interactions with algorithmic outputs may influence their behaviour as consumers, subsequently changing the way they are influenced by such outputs, and shaping their decision-making when choosing whether or not to opt-out of direct marketing. The right to object allows users to independently shape the degree to which algorithmic outputs affect them through targeted marketing, bolstering corporate accountability towards user decisions regarding how their data is used to influence them. Therefore, it should be considered a control mechanism meant to be utilized by consumers to mitigate the threat of consumer manipulation.

Vedder and Nauts (2017) highlight how "the right not to be subject to automated decision-making" is an example of "privacy and data protection as 'self-management'" (p. 216). Allowing users to choose whether or not they want to subject their personal data to processing so that algorithms can offer direct-marketing actually shifts some accountability towards individuals (Vedder & Naudts, 2017). Taken together with transparent practices evident in data subject rights that enable user awareness, the right to object appears designed to limit threats to autonomy by providing users with the opportunity to act upon the information they receive.

Likewise, Malgieri and Comandé (2017) claim that the GDPR cultivates a "legibility-by-design" system promoting "the autonomous capability of individuals to understand the functioning and the impact of algorithms concerning them" (p. 244). By creating a situation where users have control over how the processing of their data affects them, accountability can protect individuals from algorithmic effects that attempt to manipulate their consumer behaviour. The right to object to direct marketing demonstrates an accountability measure where data controllers are accountable to the direct instructions of data subjects in a process that shifts responsibility to the user as well. This accountability measure promotes user decision-making in a context where they have the ability to become informed via enforced transparent practices that enable user awareness. To address research question three, the right to object to direct marketing demonstrates how the GDPR employs practices of transparency and accountability together to promote user awareness and enable informed decision-making, which may theoretically empower users to limit threats to user autonomy.

The GDPR: Conclusions

In the case of the GDPR, principles of accountability and transparency are applied via government legislation to regulate algorithmic inputs and potentially mitigate threats to user privacy and behavioural manipulation. An in-depth analysis of the GDPR indicates that it has a strong potential to establish effective practices of accountability by creating standards for data-collection and processing, forcing organizations to inform users of their rights, and creating penalties for organizations that fail to meet such standards. As well, the GDPR fosters practices of what Weber calls procedural transparency by creating rules to force organizations to provide clear and unambiguous information to users on how their data is collected, shared, and

processed. My analysis suggests that the GDPR is designed to mitigate threats to privacy and human manipulation by first establishing methods of consent and awareness regarding how user data is collected, processed, and shared, and then by restricting the utility of such data within the permitted boundaries established by the user.

Upon considering research question one, the GDPR indicates how government legislation is capable of mitigating algorithmic threats by institutionalizing practices of accountability and transparency that corporate entities must follow when collecting and operationalizing user data via algorithms. To answer research question two, the GDPR demonstrates how practices of accountability and transparency – when built into government legislation – can theoretically limit algorithmic threats by establishing channels for active information flows, standardizing practices of control and oversight to protect user data and privacy, and creating mechanisms to facilitate user awareness and informed decision making. With regards to research question three, data subject rights regulate practices surrounding data-retention and collection to potentially diminish threats to user privacy. It does so through processes that inform users of how their data is collected and securely stored, while also enabling a degree of user control over their data. Moreover, data subject rights may also mitigate threats to autonomy because user awareness is promoted through practices of transparency; informed decision-making limits influential marketing as the GDPR's regulations enforce corporate accountability towards and among users to promote autonomy regarding how they are marketed to.

Discussion

Efficacy and the Mutual Shaping Theory

In the case of GDPR, the mutual shaping theory characterizes the government as an actor in mediating technological change. As organizations have utilized data collection and algorithms

in an unaccountable and opaque manner, European society recognizes that they pose threats to user autonomy and privacy. In line with Boczkowski's understanding of the mutual shaping theory, algorithmic capabilities and threats triggered the mediation process for the GDPR, and the GDPR recursively triggered the mediation process to alter the way algorithmic inputs are gathered via data collection practices. More specifically, algorithmic ability to manipulate users by means of data collection, processing, and direct-marketing triggered a regulatory response by the EU. Regulatory responses are also be motivated by social responses to algorithmic threats, which may be brought forward by mediating actors such as news media, advocacy groups, or users themselves.

Transparent practices include rights to access via standardized information channels to promote user awareness. Practices of accountability enforce institutionalized control and oversight mechanisms within organizations collecting and processing data, while also enabling user control over their data and interaction with algorithmic outputs. In consideration of the mutual shaping theory, transparent practices do not facilitate technical change to algorithms themselves. Rather, transparent practices and user awareness further a social capacity to shape algorithmic outputs as users make informed decisions to act upon rights that promote corporate accountability towards them. The right to have personal data deleted constrains the scope by which algorithmic inputs of user data can be collected and retained. This practice of accountability enables user control over their data – as an algorithmic input – while institutionalized oversight mechanisms encourage accountability to users within organizations. In this fashion, users shape algorithmic technology through the GDPR by affecting corporate practices of data collection and storage. Through the right to object to direct marketing, the GDPR shifts accountability to users by providing user control over how algorithmic outputs

affect them. Consumers that would otherwise be subject to influential marketing would then possess the ability to shape algorithmic functions to avoid outputs. The relationship between regulatory capacity for change, user control, and algorithmic capabilities is therefore complex and intertwined. The GDPR not only serves as a social force to shape algorithmic technology, but it also facilitates further social change to algorithmic technologies as it allows individual users to have a greater impact on algorithmic technologies through data-collection. Moreover, the GDPR allows society to shape the effects algorithmic outputs have by allowing users to exercise rights to control how practices of direct marketing – as a key algorithmic output – affect them. While the capability of algorithmic technologies shaped legislation to begin with, these technologies still have the capacity to influence consumer decision making, especially in cases where users do not take advantage of information channels and their rights to object and be forgotten.

It is also worth considering the role of algorithmic inputs in shaping the outputs that influence consumer society. Corporate design, the biases and intentions of individual creators, and user data all serve as inputs that affect the way algorithms function. In a consumer context, user data generates specific algorithmic outputs to create tailored marketing to consumers (Gal & Elkin-Koren, 2017; Mager, 2012) Therefore, shaping the parameters by which corporations are allowed to collect data is one way legislation – as a societal force – shapes the function of algorithmic technologies. Since user data is an essential input in shaping these functions, user activity online is a preliminary social force shaping algorithmic outputs which tend to reflect user profiles (Haque, 2015; Foer, 2017; Gal & Elkin Koren, 2017; West, 2017). However, user awareness of algorithmic threats may shape user activity online, which then alters the data that is collected, and subsequently changes the outputs that are produced by a particular algorithm. In

this process, the GDPR's practices to promote transparency trigger algorithmic change by increasing user awareness, which then recursively triggers the way users respond to algorithmic outputs via practices of accountability. Therefore, algorithmic functions, user inputs and responses, and government legislation are all engaged in a process of mutual shaping.

The mutual shaping theory characterizes the complex relationships between data and algorithmic regulation, users and society, and the technological capacities of algorithms, primarily because each are mutually constituted in "co-evolutionary" process (Just & Latzer, 2017). Upon considering this complex relationship of mutual shaping, the threats to consumer autonomy and privacy are theoretically mitigated by the GDPR because it enables user awareness and control in order to further the societal force in shaping the way algorithmic inputs affect users. Given that the GDPR is a facilitator of increased social control over algorithmic threats, algorithmic technologies may come to shape society in new ways. Despite the GDPR's capacity to enable social control, mutual shaping theory would suggest that algorithmic technologies will also come to shape society in new ways. In an endless cycle of mutual shaping, societal and regulatory forces may eventually loosen or tighten control over data collection and algorithmic regulation as new technological effects generate societal responses.

Socio-political Context of the GDPR

National jurisdictions are a barrier to government regulation of search engines and algorithms; the efficacy of national legislation is limited by the globalized nature of data storage and rapid access of information via the internet (Mager, 2012). The socio-political context of the EU is integral in analyzing the potential efficacy of GDPR because it contributes to the influential scope of algorithmic regulation. Since the EU is a supranational coalition, it has a

certain capacity to transcend national jurisdictions within Europe to create a cohesive policy that maintains accountable and transparent data practices among member countries. Yet the transfer of data and application of algorithms extends beyond the jurisdiction of the EU, and the GDPR is limited within Europe. Regardless of whether or not an organization operates internationally or within Europe, the GDPR "extends the jurisdictional scope of the EU's data protection laws" to any organization that monitors or interacts with users in the EU (Bhaimia, 2018, p. 24). Therefore, the GDPR can overcome the barrier of national jurisdictions to alleviate threats within the EU, but is not capable of enforcing data protection regulations for individuals outside of the EU. However, Buttarelli (2016) suggests that the GDPR can create global partnerships and an international effort to mitigate algorithmic threats by promising "wider scope for cooperation between authorities and data controllers" (p. 77). Multi-lateral initiatives have the capacity to transcend jurisdictions where organizations operate to lessen threats within the countries involved. This characteristic is relevant in discussion of potential effectiveness as it is another societal factor that shapes technological functions. The socio-political context of the EU is a social force that shapes responses to algorithmic threats, the mandate of a regulatory authority, and the scope of its influence. As a social factor in shaping practices data-collection, processing, and algorithmic functions, European society is a force recursively triggering EU legislation and therefore algorithmic technologies that effect European users.

Corporate Responses to the GDPR

Corporate algorithmic design entails that consumers are profiled in a process of "data capitalism" (West, 2017) for the purposes of marketing more efficiently to consumers in an attempt to maximize profits (Mager, 2012; Paley, 2017). We have already seen corporations

react to the changes imposed by the GDPR. LinkedIn has provided users with more "controls and choices about the data that can be used to personalize ads" and "updated language about when you allow advertisers to get access to your [the user's] personal information," noting that many of such changes were "driven" by the GDPR (Harrison, 2018). Discord, a messaging and voice chat application designed for gamers, made changes to their privacy policy in May 2018, which was "spurred" by GDPR, and noted that they are "being more specific on how we use the information we collect, how long we keep that data, and the rights you [the user] have regarding it" while "also adding information about how you can control the usage of your personal data and download the data that you've provided to us" (Discord, 2018a). In their privacy policy, Discord states that "individuals in the European Economic Area have the right to opt out of all of our processing of their personal data for direct marketing purposes," and notes the instructions on how to do so in the application (Discord, 2018b). These are only two examples among many others that identify how corporations have responded to the GDPR to allow users to access personal data, receive information about its use, and opt-out of the data-processing activities that are used to directly market to them. Although the GDPR has only come into effect recently, examples initially indicate that corporate actors have responded to meet GDPR standards. In time, further analysis may indicate if these corporate changes made in response to the GDPR will mitigate algorithmic threats as European users take advantage of their data-subject rights. Nevertheless, initial corporate responses to the GDPR indicate how government legislation is a capable social force in shaping corporate algorithmic functions and data collection practices.

While there are a number of examples of corporate responses to the GDPR, it is too early to determine how effective the GDPR will be in terms of implementation and enforcement. Based on my analysis of the GDPR in context with mutual shaping theory, the GDPR's

accountability measures should theoretically have a significant effect in regulating corporate algorithm use. As a piece of EU legislation, the GDPR forces severe financial consequences on corporations failing to adhere to the regulation, which may prove to be effective as a coercive force in regulating corporate data-collection and algorithm use. However, there already has been a marked social response to the GDPR: Facebook and Twitter have said that the GDPR is causing a drop in users and decrease in profits, despite the recent occurrence of the Cambridge Analytica scandal (Lanxon & Bodoni, 2018). The GDPR may be contributing to a shift in social perspectives that push users away from online platforms, leading to decreased revenue for big corporations relying on the activity of a high volume of users. Whether or not this is a result of increased user awareness, it is worth speculating if corporations will comply with GDPR legislation if they suffer revenue decreases beyond that of GDPR fines and penalties. As a form of governance, the GDPR is a legislative force for mutual change at an intersection between society and technology. On one hand, the GDPR acts on behalf of social responses to further the autonomy of European society as it navigates its relationship with algorithmic technology. On the other, it shapes algorithmic advancements that have risen as a result of economic forces, which have come to affect society and consumer behaviour in turn. Although the GDPR theoretically appears to be a promising force promoting European user autonomy and privacy, it will take time to determine if the GDPR's policies will be practically implemented and enforced to protect users and penalize corporations in cases of non-compliance.

Conclusion

Despite my exploration of algorithmic threats to consumer autonomy and privacy, there remain other algorithmic threats outlined by scholars, including the exacerbation of social inequalities and bias and discrimination online. In addressing the potential shortfalls of my

analysis of the GDPR, the regulations examined here do not seem to directly address algorithmic threats that exacerbate social inequalities. By regulating data collection and processing, the GDPR may make the process of data-capitalism less opaque, but there is no theoretical guarantee that this will significantly reduce power dynamics of control and exploitation of prosumer activity. Another remaining issue is that users may sacrifice some of the efficiencies of algorithmic functions by opting out of direct marketing services and data retention. Regarding algorithmic technologies and data collection, scholars have noted the trade-off that occurs as users must decide between utilizing free services and enjoying algorithmic efficiencies, or protecting their privacy and consumer autonomy (Adams, 2017; Fife & Orjuela, 2012). Based on my analysis, there is little indication as to whether the GDPR may provide an immediate solution to eliminate the trade-off between algorithmic utility and protection from privacy infringement and user manipulation. A more comprehensive analysis of the GDPR that considers conceptualizations of practices of accountability and transparency may be able to identify which specific practices outlined in the legislation may mitigate other threats posed by algorithmic technologies.

Theoretically, the GDPR should be an effective means of technological mediation where principles of accountability and transparency are put into practice. The effects government legislation has on algorithmic capabilities is important, but legislation directed at algorithmic regulation is only beginning to develop among states internationally. The empirical impact of the GDPR has yet to be determined because its implementation only occurred during the writing of this paper. Nevertheless, this paper has attempted to theoretically determine if government legislation can be an effective means of promoting social change to reduce threats to user autonomy and privacy. According to my framework, the GDPR seems capable of reducing the

algorithmic threats identified by institutionalizing open communication between data controllers and subjects to promote practices of accountability and transparency. Furthermore, transparency and the rights to access and clear terms promote user awareness to mitigate the influential capacity of algorithms and promote informed decision making. These transparent practices bolster practices of accountability as the GDPR institutes mechanisms to protect user privacy through data oversight, while also enabling user control over how their data is stored and used to market to them via algorithmic outputs. Taken together, practices of accountability and transparency are capable of mitigating threats to user autonomy and privacy, especially as they regulate data collection practices that significantly shape the capacity of algorithmic technologies in a consumer context. Overall, the GDPR may not comprehensively protect consumers from privacy threats, manipulative marketing tactics, or exacerbated inequalities and algorithmic bias, but it exemplifies a regulatory step towards corporate accountability to users that interact with their algorithms. The GDPR also has its geo-political constraints, but it demonstrates how practices of transparency and accountability can be applied to empower the average consumer and constrain corporate authority in a world where algorithmic technologies are becoming increasingly capable of influencing society.

References

Adams, M. (2017). Big Data and Individual Privacy in the Age of the Internet of Things. *Technology Innovation Management Review, 7*(4), 12–24.

Baym, Nancy K. (2015). Chapter 2: Making new media make sense. *Personal Connections in the Digital Age, 2nd edition*, Cambridge: Polity Press.

Bhaimia, S. (2018). The General Data Protection Regulation: The next generation of EU data protection. *Legal Information Management*, *18*(1), 21–28. https://doi.org/10.1017/S1472669618000051

Boczkowski P. J. (1999). Mutual shaping of users and technologies in a national virtual community. *Journal of Communication*, *49*(2), 86–108. https://doi.org/10.1111/j.1460-2466.1999.tb02795.x

Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law, 6*(2), 77-78. http://dx.doi.org.ezproxy.lib.ryerson.ca/10.1093/idpl/ipw006

Cavoukian, A. (2009). *Privacy by Design: Take the Challenge.*

Coglianese, C. (2007). Weak democracy, strong information: The role of information technology in the rulemaking process. In (Editors: Mayer-Schonberger, V. and Lazer, D.) *Governance and Information Technology: From Electronic Government to Information Government.*

Doneda, D., & Almeida, V. A. F. (2016). What is algorithm governance? *IEEE Internet Computing*, *20*(4), 60–63. https://doi.org/10.1109/MIC.2016.79

Discord. (2018a). Privacy Policy Update and GDPR FAQ. Retrieved from https://support.discordapp.com/hc/en-us/articles/360003858092-Privacy-Policy-Update-and-GDPR-FAQ

Discord. (2018b). Discord Privacy Policy. Retrieved from https://discordapp.com/privacy

European Commission. (2018). 25 May – GDPR tightens data protection rules for companies and gives people back control. Retrieved from https://ec.europa.eu/unitedkingdom/news/25-may-%E2%80%93-gdpr-tightens-data-protection-rules-companies-and-gives-people-back-control_en

Eggenschwiler, J. (2017). Accountability challenges confronting cyberspace governance. *Internet Policy Review*, *6*(3). https://doi.org/10.14763/2017.3.712

Equifax. (2017, September 7). Equifax Announces Cybersecurity Incident Involving Consumer Information. Retrieved from https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628

Fife, E., & Orjuela, J. (2012). The Privacy Calculus: Mobile Apps and User Perceptions of Privacy and Security. *International Journal of Engineering Business Management*, *4*, 1-11.

Flyverbom, M., Deibert, R., & Matten D. (2017). The governance of digital technology, big data, and the Internet: New roles and responsibilities for business. *Business & Society*. https://doi.org/10.1177/0007650317727540

Foer, F. (2017). *World without mind: The existential threat of big tech*. New York: Penguin Press.

Fountain, J. E. (2007). Challenges to organizational change: Multi-level integrated information structure (MIIS). In Mayer-Schonberger, V. and Lazer, D. (Eds.), *Governance and Information Technology: From Electronic Government to Information Government.*

Gal, M. S., & Elkin-Koren, N. (2017). Algorithmic consumers. *Harvard Journal of Law & Technology*, *30*(2), 309-353. Retrieved from http://link.galegroup.com.ezproxy.lib.ryerson.ca/apps/doc/A503308835/AONE?u=rpu_main&sid=AONE&xid=41df0073

Gasser, U., & Almeida, V. A. F. (2017). A layered model for AI governance. *IEEE Internet Computing*, *21*(6), 58-62.

https://doi-org.ezproxy.lib.ryerson.ca/10.1109/MIC.2017.4180835

General Data Protection Regulation. (2016). *Official Journal of the European Union, 59.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

GDPR FAQs. (2018). *EU GDPR Portal.* Retrieved from https://www.eugdpr.org/gdpr-faqs.html

GDPR Timeline of Events. (2018). *EU GDPR Portal.* Retrieved from https://www.eugdpr.org/gdpr-timeline.html

Hale, T. (2008). Transparency, Accountability, and Global Governance. *Global Governance, 14*(1), 73-94. Retrieved from http://www.jstor.org/stable/27800692

Haque, A. (2015). Chapter 4: Leadership, Ethics, and Technology. *Surveillance, transparency, and democracy: Public administration in the information age.* Retrieved from https://ebookcentral-proquest-com.ezproxy.lib.ryerson.ca

Harrington, S. (2018, March 8). Updates to our Terms of Service. *Linkedin Official Blog.* Retrieved from https://blog.linkedin.com/2018/march/8/updates-to-our-terms-of-service

Henning, P. J. (2017, December 22). Hack will lead to little, if any, punishment for Equifax. *The New York Times*. Retrieved from https://www.nytimes.com/2017/09/20/business/equifax-hack-penalties.html

Just, N., & Latzer, M. (2017). Governance by algorithms: Reality construction by algorithmic selection on the Internet. *Media, Culture & Society, 39*(2), 238–258. https://doi.org/10.1177/0163443716643157

Lanxon, N., & Bodoni, S. (2018, July 27). Facebook, Twitter Say Europe's Privacy Law Causing User Drop. *Bloomberg.* Retrieved from https://www.bloomberg.com/news/articles/2018-07-27/facebook-says-eu-privacy-law-caused-user-drop-europe-disagrees

Mager, A. (2012). Algorithmic ideology: How capitalist society shapes search engines. *Information, Communication & Society, 15*(5) 769–787. http://dx.doi.org/10.1080/1369118X.2012.676056

Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the general data protection regulation. *International Data Privacy Law, 7*(4), 243-265. doi:10.1093/idpl/ipx019

Mann, G., & O'Neil, C. (2016, December 9). Hiring algorithms are not neutral. *Harvard Business Review.* Retrieved from https://hbr.org/2016/12/hiring-algorithms-are-not-neutral

McKelvey, F., Tiessen, M., & Simcoe, L. (2015). A consensual hallucination no more? The Internet as simulation machine. *European Journal of Cultural Studies*, *18*(4–5), 577–594. https://doi.org/10.1177/1367549415584856

Paley, Norton. (2017). Chapter 1: Developing Effective Leadership: The Human Interface with Big Data, Algorithms, and Analytics. *Leadership Strategies in the Age of Big Data, Algorithms, and Analytics.* Productivity Press.

Puzzanghera, J. (2018, January 10). Senators want "massive" fines for data breaches at Equifax and other credit reporting firms. *Los Angeles Times.* Retrieved from http://www.latimes.com/business/la-fi-equifax-data-breach-fines-20180110-story.html

Quan-Haase, A. (2015). *Technology and society: Social networks, power, and inequality*. Oxford University Press.

Saurwein, F., Just, N., & Latzer, M. (2015). Governance of algorithms: Options and limitations. *Info*, *17*(6), 35–49. https://doi.org/10.1108/info-05-2015-0025

Sreejesh, M., Anusree, M. R., & Amarnath, M. (2016). Effect of information content and form on customers' attitude and transaction intention in mobile banking: Moderating role of perceived privacy concern. *The International Journal of Bank Marketing; Bradford*, *34*(7), 1092–1113.

Summary of Articles Contained in the GDPR. (2018). *EU GDPR Portal.* Retrieved from https://www.eugdpr.org/article-summaries.html

Van Loo, R. (2017). Rise of the digital regulator. *Duke Law Journal, 66*(6), 1267-1329. Retrieved from http://link.galegroup.com.ezproxy.lib.ryerson.ca/apps/doc/A491611238/AONE?u=rpu_main&sid=AONE&xid=c34d3f72

Vedder, A., & Naudts, L. (2017). Accountability for the use of algorithms in a big data environment. *International Review of Law, Computers & Technology, 31*(2), 206-224. doi:10.1080/13600869.2017.1298547

Weber, R. H. (2008). Transparency and the governance of the Internet. *Computer Law & Security Report*, *24*(4), 342–348. https://doi.org/10.1016/j.clsr.2008.05.003

Weber, R. H. (2011). Accountability in the Internet of Things. *Computer Law & Security Review*, *27*(2), 133–138. https://doi.org/10.1016/j.clsr.2011.01.005

West, S. M. (2017). Data Capitalism: Redefining the logics of surveillance and privacy. *Business & Society*. https://doi.org/10.1177/0007650317718185

Yanofsky, N. S. (2011). Towards a definition of an algorithm. *Journal of Logic and Computation*, *21*(2), 253–286. https://doi.org/10.1093/logcom/exq016