June 2021

Asymmetrical Governance: Auditing Algorithms to Preserve Due Process Rights

Paul J. Baillargeon
baillarp@uwindsor.ca

Asymmetrical Governance:

Auditing Algorithms to Preserve Due Process Rights

by

Paul Baillargeon

A Major Research Paper

Submitted to the Faculty of Graduate Studies

Through the Department of Communication, Media and Film

in Partial Fulfilment of the Requirements

for the Degree of Master of Arts at the

University of Windsor

Windsor, Ontario, Canada

Asymmetrical Governance:

Auditing Algorithms to Preserve Due Process Rights

by

Paul Baillargeon

APPROVED BY:

_____

B. Brown

Department of Communication, Media & Film

_____

V. Manzerolle, Advisor

Department of Communications, Media & Film

May 19, 2021

DECLARATION OF ORIGINALITY

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

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

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

ABSTRACT

We are now living in age where algorithms, and the data that feed them, govern a wide variety of decisions in our lives: not just search engines and personalized Netflix suggestions, but educational evaluations, stock market trades and political campaigns, the urban planning, and even how social services like welfare and public safety are managed. Heterogeneous lists like this have become the norm in any critical examination of algorithms, giving the impression of a ubiquitous relevance of algorithms. But algorithms can make mistakes that directly affect individuals and often contain both implicit and explicit biases. The technical complexity of algorithms, the scale at which they operate, and their proprietary nature makes them difficult to scrutinize, creating challenges to fully comprehend of how they exercise their power and influence over society. When used to make legal decisions, questions must be asked as to how automated decision-making systems affect the right to due process afforded to citizens.

The goal of this research project is to augment this discussion by focusing on algorithmic transparency, due process rights, and what can be done to help protect said rights when automated decision-making systems are used. Therefore, the research question that guides this paper is as follows: *In what ways do algorithms in legal processes negatively impact an individual's right to due process and how might the ability to audit legal algorithms help protect due process rights?*

To answer this question this research project will present recommendations for research methods, adapted from Communication scholar, Christian Sandvig's proposed research methods (2014) that can be utilized to audit algorithms so as to provide greater transparency to those on the receiving end of algorithmic judgements within the legal process.

ACKNOWLEDGEMENTS

I would like first to express my love and sincere gratitude to my partner Johanna Dennie, without her patience for my procrastination and subsequent encouragement for me finish this research I may have never gotten to this point. The Pandemic has been hard on all of us and with her love and support I was able to overcome any doubt I once had.

I would also like to express heaps of thanks to my supervisor Dr. Vincent Manzerolle for his support, enthusiasm, and guidance through the process of my M.A. He has been a constant source of inspiration throughout most of my time at the University of Windsor and is one of the first people to get me exited about communication studies. I would also like to thank my Faculty reader Dr. Brian Brown providing me with valuable insights and useful remarks for what once seemed like a daunting task.

TABLE OF CONTENTS

DECLARATION OF ORIGINALITY iii

ABSTRACT iv

ACKNOWLEDGEMENTS v

INTRODUCTION 1

CHAPTER 1

ALGORITHMIC POWER IN SOCIETY 3

THE NON-NEUTRALITY OF ALGORITHMS 8

CHAPTER 2

THE ALGORITHMIC BLACK BOX 12

BLACK BOXES AND DUE PROCESS RIGHTS 16

CHAPTER 3

CASE STUDIES 22

IMMIGRATION, ALGORITHMS, AND DUE PROCESS 23

BAIL, PRE-TRIAL RISK ASSESSMENTS, AND TRANSPARENCY 26

CHAPTER 4

AUDITING DECISION-MAKING ALGORITHMS 32

CODE AUDIT (ALGORITHM TRANSPARENCY) 34

SCRAPING AUDIT 36

CONCLUSION 39

REFERENCES 42

VITA AUCTORIS 51

Introduction

We are now living in age where algorithms, and the data that feed them, govern a wide variety of decisions in our lives: not just search engines and personalized Netflix suggestions, but "educational evaluations, the operation of markets and political campaigns, the design of urban public spaces, and even how social services like welfare and public safety are managed" (Diakopoulos, 2015. p. 398). Heterogeneous lists like this one by Diakopoulos (2015) have become the norm in any critical examination of algorithms, giving the impression of a ubiquitous "relevance of algorithms" (Gillespie, 2014). But algorithms can make mistakes that directly affect individuals and often contain both implicit and explicit biases. The technical complexity of algorithms, the scale at which they operate, and their proprietary nature makes them difficult to scrutinize, creating challenges to fully comprehend of how they exercise their power and influence over society.

More specifically, the use of algorithmic systems in society has continued to grow steadily over the last decade, with their use expanding beyond the everyday digital media platform or search engine and into various federal and corporate institutions that govern the lives of individuals. By making their way into the governing bodies of society, algorithms must be critically examined within different frameworks in order to unravel the complex web of consequences they might have on the individuals they are tasked with governing. When used to make legal decisions, questions must be asked as to how automated decision-making systems affect the right to due process afforded to citizens. Due process is the legal requirement that the government must respect all legal rights a person is owed, such as a "fair and open procedure, appropriate to the decision being made and its statutory, institutional, and social context, with an opportunity for those affected by the decision to put forward their views and evidence fully and

have them considered by the decision-maker" (Hildebrandt, 2016. p. 100). While due process is used in criminal law, procedural fairness is equitable to due process, but for administrative law. This MRP will use due process to refer both due process and procedural fairness for ease of understanding as they are very similar terms.

While discussions surrounding the topic of algorithms and the algorithmic have been incredibly varied, spanning over multiple research disciplines, such as computer science, communications, and critical legal studies, the question remains: in what ways do algorithms in legal processes negatively impact an individual's right to due process and how might the ability to audit legal algorithms help protect due process rights? In order to address this gap in existing literature, this MRP will be presented in four chapters that focus on algorithmic transparency and how it relates to an individual's due process rights.

Chapter 1 will look at the extant literature surrounding the ways algorithms exercise power, their politics and biases embedded within them. By examining the ways in which people experience algorithms in everyday life and the ways in which these algorithms have the potential to shape individuals' experiences, the perceived neutrality of algorithms is brought into question. This chapter will use explore the non-neutrality of algorithms as value laden artifacts to demonstrate their potential for biased decision making.

Chapter 2 will explore the problem of their black box nature, and the effects this has on an individual's legal right to due process. The concept of the black box is essentially a catch-all term for the things that cannot be fully understood; this term has become often used when referring to the inner workings of algorithms. The inability to fully understand the process by which an algorithm makes it decisions is antithetical to the right to due process. By discussing

Citron's (2008) technological due process framework, the implications of transparency and fairness within algorithmic legal process will be unpacked.

Chapter 3 will discuss two separate legal processes in which algorithms are used to make legal decisions and how those processes affect an individual's right to due process. Firstly, the use of decision-making algorithms in the field of immigration law will be examined to demonstrate the effect of algorithmic decision-making systems have on administrative legal processes. Secondly, the use of algorithms to make risk assessments in bail hearings will be discussed to show that while the algorithms and procedures may differ, much of the same algorithmic challenges arise in criminal law as they do in administrative law.

Finally, Chapter 4 will present recommendations for research methods, adapted from Communication scholar, Christian Sandvig et al's proposed research methods (2014) that can be utalized to audit algorithms so as to provide greater transparency to those on the receiving end of algorithmic judgements within the legal process. Of the 5 proposed audit types Sandvig et al proposes Code Audit (Algorithm Transparency) and a Scraping Audit are the two that will be explored. It will be argued that by providing procedures for auditing algorithms, an individual's due process rights may be preserved even in the event of an algorithmic decision-maker.

Chapter 1

Algorithmic Power in Society

The term algorithm has come to be understood differently depending on the perspective from which they are encountered. Technical specialists, social scientists, and the broader public each use the term in different ways (Gillespie, 2016. p. 19). Bucher (2018) refers to this when she states that algorithms are multiple "in the sense that the term algorithm refers to more than

one kind of thing" (p. 19). Gillespie (2016) mentions that for the makers of algorithms, that is the computer scientists who code them, "the term refers specifically to the logical series of steps for organizing and acting on a body of data to quickly achieve a desired outcome" (p. 19). Whereas the general public sees them as absurdly complex digital objects. Succinctly, "an algorithm is a recipe composed in programmable steps; most of the "values" that concern us lie elsewhere in the technical systems and the work that produces them (Gillespie, 2016. p. 19). However, while this may work for a definition of algorithm in the form of a noun, algorithm is often used as a verb by social scientists when they refer to something as algorithmic. Gillespie (2016) points out that what makes something algorithmic "is that it is produced by or related to an information system committed (both functionally and ideologically) to the computational generation of knowledge or decisions" (p. 25).

Much of the recent discourse around algorithms in the social science has focused on two key themes: i) algorithms as powerful political actors whose operations bear consequences in a multiplicity of domains and ii) the difficulty of explaining or knowing precisely how algorithms exercise their power and influence (Ziewitz, 2016). Due to the power and consequences imbued in algorithms it has been argued that due to the ubiquity of algorithmic computing devices in everyday life there is a crucial need to better understand the human-machine dynamic that algorithms have within society (Gillespie, 2014; Kitchin, 2016; Willson 2016). Algorithms facilitate an ever-growing list of tasks in the world, many of them simultaneously: they effortlessly search information, categorize and group individuals, profile people digitally, and have a hand in managing just about any aspect of present-day life (Cheney-Lippold, 2011).

The sheer pervasiveness of computerized systems, or "algorithm machines" as Gillespie (2014) refers to them, has left society with a newfound, yet uninformed, reliance on these

systems. These algorithmic machines are entrusted with everything, from the mundane practices of everyday life such as searching the web (Willson, 2016, Bucher, 2018), to dealings of large corporations like financial institutions(Pasquale, 2015), to determining if an individual should make bail (Angwin, 2016). Wilson (2016) sees the ubiquity of algorithms in the present day as a "synergistic melding of human and machine" (Willson, 2016. p. 143). There is a plethora of documented examples by scholars in fields such as computer science, communications, and critical legal studies that research the synergistic melding of human and machine at all levels of society; individuals, corporations and governments are all attempting to delegate as many tasks as possible to these algorithmic machines in order to maximize time and money (Eubanks, 2018; Karppi, 2015).

At the individual level there is an algorithmic interplay with peoples' social lives, as Beer (2009) states, algorithms "have the capacity to shape social and cultural formations and impact directly on individual lives" (p. 994). The consequence of this Beer (2009) continues "is that we are now faced with a new set of rules to live by" (p. 994). There is no better example of this algorithmic social shaping and its consequences on the individual's everyday experience than social media giant Facebook. On Facebook the very notion of how relationships are formed, structured, and sustained is changing; the very concept of friendship is developing new meaning alongside that of society's traditional understanding of friendship and all of its nuanced practices. Rather than having a traditional understanding of what friendship means, users of social media are having to understand the societal norms and expectations of digital friendship, how these digital friendships interplay with our traditional understanding of friendship, and what is the proper balance between two (Bucher, 2012). For Bucher, Facebook's algorithms have created friendships that involve numerous human and non-human actors, relationships that rely on the

dynamics between a person and software, and are not always completely voluntary (Bucher, 2012).

At the corporate level algorithms are being used to collect as much personal information as possible, from every device imaginable, in order to categorize consumers into neat and orderly groups so that advertisers can better target their audiences (Srnicek, 2016). These categories, based on individuals' web history, online shopping habits, and other online activities make up what Cheney-Lippold (2011) terms our "algorithmic identity" (p. 165). Advertisers use these new algorithmic identities to guide, influence, and persuade our online habits; these algorithmic identities in turn end up informing our understanding of the physical world (Cheney-Lippold, 2011). Algorithms possess the ability to sort through and categorize information autonomously and rapidly in ways that humans simply could not keep up with.

Srnicek (2016) has covered the shift businesses and industries are making in order to incorporate the earnings and savings potential of algorithms. Entirely new digital industries are quickly coming to dominate the top grossing corporations in the world built on algorithmic software; whether it be new digital platforms like Facebook and Amazon or older industries like advertising or news distribution, all are adapting to an algorithmic and data driven "platform capitalism" (Srnicek, 2016). The industrial adoption of algorithmic processes is directly tied to their success as their "businesses, and their products depends heavily on the synthesis of data and perceptions into reputation" (Pasquale, 2015. p. 14).

Lastly, at the governmental level, algorithms have been combined with surveillance tactics and used to gather data on citizens. Whether it is the use of location data (Murphy, 2017), internet browser history (Cheney-Lippold, 2011) or any of the numerous other ways that individuals create mineable metadata, the government can and likely will collect as much of it as

possible (MacAskill, E., & Dance, G. 2013). The instantaneous nature in which algorithms process data behind the scenes is largely seen as a positive rationale for their use in a variety of industries and administrative settings. The speed at which algorithms calculate, configure, and sort information far exceeds the capacity of human cognitive capabilities, thus allowing for cost saving measures by employing the use of algorithms instead of paying human labourers (Srnicek, 2016. p. 49).

The seemingly inherent financial benefit of using algorithms has made them exceptionally enticing to both the Canadian and American administrative branches of government that are responsible for social services like healthcare, welfare and food-stamps, child protective services (Eubanks, 2018), and immigration (Molnar & Gill, 2018) due to the sheer volume of cases these types of services deal with. Over the course of the twentieth centaury these administrative branches of government were expanding in size while also "wield[ing] ever-increasing power, implementing comprehensive regulatory programs and distributing benefits to tens of millions of people" (Citron, 2008. p. 1251).

Virginia Eubanks (2018) examines the ways in which the introduction and use of computational systems such as decision-making systems and ranking algorithms are used within various social services in the US and how these systems have a detrimental effect on those whom they purport to help. Eubanks examined three different social services, healthcare/food stamps/cash benefits in Indiana, housing for the homeless in Los Angeles, and child welfare in Pittsburgh. In each case Eubanks began with interviews of people whose lived experience has been directly affected by the services to be explored. In the case of Pittsburgh child protective services, Eubanks explains how the algorithmic system used to help predict if a child is at risk of neglect only collects partial data, "missing key factors that influence abuse and neglect" (p.146).

When an algorithm is missing data points on key factors, it is “guaranteed to produce thousands of false negatives and positives” since “a model’s predictive ability is compromised when outcome variables are subjective” (Eubanks, 2018. p. 146). However, the non-neutrality of algorithms is not something that can be easily removed.

The Non-Neutrality of Algorithms

While algorithms may be ubiquitous, they are by no means neutral or objective bystanders. Technology “in itself is neither good nor bad, but it is never neutral” (Hildebrandt, 2009, p. 451). The non–neutrality thesis of technology claims that every technology “invites certain behaviours and inhibits others, or even enforces certain behaviours while prohibiting others” (2009, p. 451). This means that before we can make moral assessments of a specific technology, or even entire technological systems, the normative implications of a technology must first be investigated. Winner (1980) famously argued for the non-neutrality of technology by using the example of a Long Island low sitting highway overpass. The overpass was situated low enough that busses were unable to pass under the bridged highway, the road that passed under the overpass was the only method of travel to a specific location of the city, effectively cutting off that part of the city to bus patrons (Winner, 1980). Winner points out that those who rely on bus transportation are often poor or racialized individuals, thus the overpass becomes a technological barrier that allows for the discrimination of certain groups of people, non-white folks. The overpass effectively made a part of the city for white people only without creating any new discriminatory law, but rather using a piece of physical infrastructure to indirectly discriminate against whole populations of people. While Winner’s example is contested by some, the main point that objects have politics still stands (Joerges, 1999).

The non-neutrality thesis applies to all technologies, meaning the algorithms that populate our digital world are not neutral tools, but value laden objects capable of both producing culture and shaping our perceptions of it (Nobel 2018). The values entangled within the coded architecture of automated systems has been well documented, from online search results (Baker and Potts, 2013; Nobel, 2012, 2018; Diakopoulos, 2013) and personalized online recommendations (Datta et al, 2015; Van-Dijck, 2013), to human recognition software (Carty, 2011; Introna, 2004; Tatman, 2016) and social services (Eubanks, 2018). According to Kitchin (2016) in order to better understand the possible effects and consequences of automated systems they must be framed within the wider context of their socio-technical assemblage. This is to say, that examining the coded language that makes up an algorithm's internal logic might not ever fully explain the consequences they have on peoples lives. The interaction between the technology and the people must be considered in tandem, as an assemblage of many individual factors.

Sofia Noble has researched the non-neutrality of algorithmic media, with a focus on search engine racial biases, as well as the potential harms these big-data biases may have on individual and group identities. She dissects the discriminatory biases that are coded into the systems themselves as these encoded prejudices perpetuate and amplify negative social stereotypes. Noble's work makes evident the ways racial biases are socially constructed by or within technology by demonstrating how black women are often portrayed in search results as pornographic objects, yet the search results themselves are suggested to be both neutral and representative of society by the engineers who coded the system (Noble, 2018, pp. 17-19). The engineers claim that the systems are not biased and that the results are reflections of what is most popular in society (Noble, 2018, p. 60), ignoring the implicit and explicit biases that may be held

by coders of the system that may find their way into the algorithmic architecture of a search engine. The biases that are baked into the search engines control how representations of identity are understood in society, for example a search for unprofessional hair styles returned images of hair styles commonly found on women of colour, whereas a search for professional hair cut returned images of white women (Noble, 2018, p. 83). Kitchin (2016) aligns with Noble's claim that algorithms can inform our understanding of society they state that algorithms "shape how we understand the world and they do work in and make the world through their execution as software, with profound consequences" (p. 18).

Given the rapidly growing importance of algorithmic ranking systems and other aggregators of information like Google, Pasquale (2006) argues that algorithms reflect "actual human judgment" (p. 117) and should not be seen as devoid of human values. Automated systems are claimed to process all individuals in the same way, thus averting discrimination. But this understanding is misleading according to Citron & Pasquale (2014), "because human beings program predictive algorithms, their biases and values are embedded into the software's instructions, known as the source code and predictive algorithms" (p. 4). Friedman and Nissenbaum (1996) developed a framework for understanding bias within a computer system; the framework described three primary types of biases: i) Pre-existing bias, ii) technical bias, and iii) emergent bias. Each of these three forms of bias manifest in different ways.

First, pre-existing biases are coded into the system either consciously or unconsciously. An example of this would be Winner's (1980, p. 23) over-pass or the discriminatory pricing used by the Princeton Review (Angwin et al., 2015) to over-charge Asian American's on standardized tests, selling them at almost twice the cost of what non-Asian Americans. Second, technical bias occurs out of the technical limitations or operational restrictions a system may have. This type of

bias occurs when algorithms do not place the same value on specific groups or individuals when it has no reason not to. For example, Facebook's discriminatory housing ads (Benner et at, 2019) where advertisers were actively given the option to target ads based on religion, therefore allowing for discriminating against specific groups. And thirdly, emergent bias refers to biases that are created by the users of an algorithmic system after it has been released to the public or user base. This could be found in almost any case where machine learning algorithms are used to understand the patterns of users, as the users can begin to manipulate the algorithm once they understand how it generates its data. Microsoft's AI chat bot Tay is a perfect example of emergent bias. Tay was a AI chat bot meant to converse with people on twitter in real time to gain valuable information on how the algorithm powering Tay processed human language. What Microsoft did not consider was that people would quickly begin to feed Tay racist and problematic language and since Tay would create its responses using previous conversation data it began regurgitating the inflammatory and offensive language fed to it (Vincent, 2016). Each of these types of biases can be either implicit or explicit, depending on the intentions behind their implementation into the systems.

In general, the scholarly communication and media literature that address algorithms agrees that they are cultural artifacts that work with and in society They act as tools that in some instances may be beneficial, but in others, detrimental to particular groups.[1] Essentially, the lines of code that are the underlying instructions for an algorithm's functioning are in fact its own culture-shaping artifact, meaning it is separate from the interface in which it operates, for

[1] While not explicitly discussed in this MRP the topic of bias facial recognition algorithms, particularly in relation to black people, is a good example algorithmic bias and its impacts on different groups. Often the data sets used to program facial recognition software includes a majority of white skin tones as opposed to an even mix of light and dark skin tones. This causes the software to have a much higher error rate when used on black people (Introna, 2004).

example Facebook, Google or the computer itself (Cheney-Lippold, 2011). The algorithm is merely an infrastructural component of the overall system in which it is incorporated. With the understanding that algorithms both produce culture and have agency within it, the literature seems to echo Kitchin's (2016) claim that algorithms ought to be examined within the wider context of their socio-technical assemblage if they are effects are to be fully understood.

Chapter 2

The Algorithmic Black Box

While there is a growing scholarly consensus around the agency and power algorithms possess, the ability to analyze the inner workings and logics that inform an algorithm's inputs and outputs comes with its own unique challenges. One barrier faced by those who study the societal implications of algorithms is their proprietary nature (Pasquale, 2015. p. 4). Platforms such as Facebook's, Google's, or even the ones that police use in their attempts at predictive policing (Ferguson, 2017), are all proprietary and are the property of the corporations that are responsible for either the coding or the licensing of the algorithm (Pasquale, 2015. p. 4). This means that the coded lines of text that powers an algorithm are the intellectual property (IP) of the company that produces it, in the same way the patented design of a Dyson Vacuum cleaner are protected under IP laws. Many scholars refer to algorithms of this nature as "black boxes," since we only see the input information that is fed into the algorithm and the resulting data form its output. There is, then, little clarity of the inner workings of these algorithms or how their results came to be (Cheney-Lippold, 2011; Diakopoulos, 2014; Kitchin 2016).

The concept of the black box is a catch-all term for things that cannot be fully identified, referring to an opaque technical device where only the inputs and outputs can be understood and

the process itself is unknowable. The use of the black box metaphor is not something that is only ascribed to algorithms and has often been used to describe everything from the brain to markets to nation states (Bucher, 2018, p. 42). However, for the purposes of this research the black box will specifically be used to conceptualize the problem of the algorithmic unknown. This is not an unknown in the sense that one lacks knowledge or information, but rather something "that if given the right resources, might be knowable in principle" (Bucher, 2018, p. 43). This type of unknown is often referred to as a "knowable known unknown" (Bucher, 2018, p. 43).

While the traditional understanding of a black box sees both input and outputs as knowable, in some instances of algorithmic black boxes, only the outputs are able to be known by the user and the inputs are unbeknownst (Diakopoulos, 2014). Google's auto complete is representative of when both the input and the output can be known; a user is able to input their search query (input) and see the search results that the search algorithm suggests (output). In the case of an algorithms input being unknowable, an example of this would be the algorithmic assessment of students work by the Turnitin system (Introna et al, 2016). The input data taken from a student's work after they have submitted to the system is unknown to the student, they are at most only able to see the plagiarism score that the program assigns them, never the criteria that led to the formulation of the score (Introna et al, 2016). If the code that makes up the logic and procedural functioning of the algorithm are exposed the system can be gamed by individuals, not to mention the code could be replicated diminishing any value the original may have had. Pasquale (2015) refers to the black box and proprietary nature of algorithms as a "one-way mirror" of knowledge (p. 9).

The asymmetry of knowledge that algorithms create is only one part of the overall issue of transparency; once access has been granted to peer inside the black box of the algorithm

individuals scrutinizing them must be able to understand what they are seeing. Perel & Elkin-Koren (2017) state that "Algorithms are non-transparent by nature; their decision-making criteria are concealed behind a veil of code that we cannot easily read and comprehend (p. 181)." Grimmelmann (2005) explains, via the example of IBM's chess playing computer Deep Blue, that it may even be impossible to fully understand how algorithmic systems come to the decisions they do because the sheer volume of information they are able to process greatly exceeds human capacity. For Deep Blue to decide to make a move it processes thousands upon thousands of other potential moves in order to conclude why the one it made was the most optimal (Grimmelmann, 2005). Those who designed the software may not be aware of the biases embedded in the systems or have the knowledge to understand them, whereas those who may be more adept at studying biases in computer systems may not be as well versed in deciphering the densely written code (Bucher, 2018).

Additionally, algorithms are often dynamic in their ability to adapt and evolve depending on the data they are fed and the patterns they identify from it (Ziewitz, 2016). Wilson (2017) states that algorithms' "multiplicity and complexity, their embeddedness in many online processes, and the mundane nature of much of what they do," as well as their "requirement for technical knowledge or literacy that many people lack when dealing with often complex mathematical and technical systems" (p. 10) create barriers for understanding how they function within a given technical system. The challenge of deciphering an algorithms code further makes them unpredictable to users, researchers, and even those who work on the code itself. Bucher (2018) argues something similar, while also emphasizing the non-static, always-changing manner in which algorithms are deployed. Bucher uses the example of Netflix A/B testing to demonstrate how Netflix can have multiple of the same algorithms running at that same time so

that it can determine which version best suits the task at hand (Bucher, 2018. p. 48). A/B testing is a method used by internet platforms to test which iteration of an algorithm suits their desired need best by testing them along side each other. For example, Netflix, in an effort to improve their recommendation algorithm will have two sets of users using two different algorithms and then measure variables like “time spent watching vs. time spent searching” and see which version of the algorithm achieved better results.

The black box problem surrounding algorithms is not changing any time soon, which has led Beer (2017) to claim that in order to address “the social power of algorithms, we would, of course, point to the need to continue to look inside the black box” (p.10) or “black box society” as Pasquale (2015) refers to it. Beer (2017) argues that we need to look inside the algorithmic systems in order to understand their technicalities, as well as potential for social ordering. However, this code analysis must also be accompanied by studies of how those algorithms operate in practice (Beer, 2017. p. 11). Examining how algorithms mesh into the fabric of organisations and institutions Bucher (2018) echo’s Beer’s thoughts and calls for “unknowing of algorithms” (p. 46). To unknow an algorithm stems from our desire to know what an algorithm is. That is, what are the specific lines of code that allows an algorithm to function, what informs the algorithm’s decision making? To unknow an algorithm according to Bucher does not imply “black boxing the black box even further” but rather means “seeing differently, looking elsewhere, or not even looking at all” (2018, p. 46). Unknowing is akin to taking what is familiar and making it less familiar; in this case algorithms can mean different things to different disciplines. For example, an algorithm to a computer scientist might be understood as a unbiased mathematical formula for processing complex equations, where as a communications researcher may view algorithms as digital recommendation systems that perpetuate the biases of those who

wrote the code. In an effort to understand their multiplicity it is important to consider alternate perspectives. This is not asking for computer scientists, social scientists, or legal technology scholars to dismiss their knowledge, but instead to asks them to take a step back and consider the varied interpretations of what it means to know an algorithm.

Black Boxes and Due Process Rights

When algorithms are used in legal processes and governmental institutions questions must be asked as to how automated systems affect the right to due process afforded to citizens. Legal scholars such as Danielle Keats Citron (2008) argue that the new dynamic brought upon by the inclusion of algorithms in legal processes requires a new understanding of due process, one Citron terms "technological due process" – "procedures ensuring that predictive algorithms live up to some standard of review and revision to ensure their fairness and accuracy" (Citron, K. & Pasquale, F., 2014). Technological due process has two primary goals: firstly, protecting individual rights by assuring adequate notice of decisions are given to defendants, and secondly, by making sure fair hearings are had by educating hearing officers to correct any machine bias.(Citron, 2008)While the term "automated decision-making systems" is used by Citron and many other scholars cited in this MRP to account for how algorithms are operationalized in a judiciary setting it is important to note that this term is often used interchangeably with other technical definitions. Automated decision-making systems process information in the form of input data using an algorithm (or algorithms) to generate an output of some kind and are therefore often used synonymously with the terms like algorithmic prediction, predictive analytics, and automated prediction (Molnar & Gill, 2018). For example, algorithms used in legal processes that determine if a defendant should be released on bail might process input data like number of prior offences, types of prior offences, length of time between offences, as well as

basic information such as age, family background, or where a person lives. These data points, along with countless others, are processed by an algorithm which then outputs a risk assessment score that is meant to assist a judge in making unbiased decisions on whether or not a defendant makes bail.

Citron's (2008) technological due process framework is used to partially replace aspects of adversarial justice that automation renders ineffectual, such as opportunities to be heard and meaningful notice. Citron recognizes the non-neutral nature of algorithms and the harmful discriminatory biases that can be encoded within them. Similarly, Pasquale (2015) argues that "values and prerogatives that the encoded rules enact are hidden within black boxes"; this is concerning, because "authority is increasingly expressed algorithmically" (p. 8). This means that the laws and procedures that govern society are increasingly being concealed within algorithms making it difficult to challenge their judgements or check for potential discriminatory practices. Understanding the non-neutrality of algorithms Citron' (2008) technological due process framework attempts to both recognize the potential benefits that algorithms bring to legal and administrative processes, while at the same time accounting for the potential harms they might bring. Being able to understand, prevent, and challenge potential biases within legal decision-making algorithms and to ensure that they do not inhibit an individual's access to their due process rights is necessary if use of said algorithms is to continue in an ethical fashion.

The speed and efficiency with which algorithms covertly process data is considered beneficial within a variety of governmental, bureaucratic, and administrative settings. The seemingly inherent financial benefit of using algorithms has made them exceptionally enticing administrative branches of government that are responsible for social services like health-care, welfare and food-stamps, child protective services due to the sheer volume of cases these types

of services deal with (Eubanks, 2018). Along with social services, governments are seeing financial benefits in using algorithms to reduce case loads in areas of law that are known to have significant backlog, such as immigration law (Molnar, P. & Gill, L., 2018), thus reducing the amount of time and labour costs it takes to process the sustained flow of new cases.

While many governmental and administrative programs like the ones studied by Eubanks (2018) enjoyed varying degrees of success before the implementation of algorithms into their infrastructure, they were often criticized for having unaccommodating rules, serious backlogs, and unfair adjudicatory practices (Molnar & Gill, 2018). In order to address any complaints against these services more personnel with and without experience would have to be hired and more money budgeted towards these growing government agencies. This is where algorithmic systems are factored in, as noted by Citron (2008), "because automation radically reduces the human role in executing government policy and programs, state and federal governments can cut staff and close field offices" (p. 1252). Advocates of algorithmic automation argue that decisions become more consistent due to the perceived neutrality of computer systems, since computers "interpret rules in the same way for every case" (Citron, 2008. p. 1253). This belief is commonly understood as misinformed, making it vital that the use of any technological system to affect the civil liberties of an individual be viewed as a non-neutral entity as mentioned previously (Hildebrandt, 2009).

As misinformed as it may be, the hearing officer or judge of a case may be biased towards a computer system and can affect the case even if the hearing officer, who is to be making the final decision on the case, is impartial to the people presenting their case (Citron 2008). The hearing officer or judge's potential belief that the decisions made by a computer system are error proof and free of any bias can negatively impact the fairness of the hearing. The

perception of error-proof, automated decisions leads to a greater likelihood of an error in judgment from the hearing officer occurring during the proceedings. Courts typically address issues of prejudice when officers have personal connections to individuals appearing before them or other conflicts of interest. However, Citron (2008) notes that "officers who have no disqualifying personal connection with individuals but who are influenced by automation bias might endorse inaccurate computer decisions even in the face of contrary evidence. Under present conditions, the guarantee of an impartial reviewer may be illusory" (p. 1284). Similarly, while not in a legal setting, Introna et al. (2016) argue that by using the Turnitin software professors and tutors are placing faith in a system they see as a neutral tool that simply detects plagiarism; "in other words, they do not trust their own expertise and judgment but rather accept the authority of the algorithm to be objective" (p. 39). If this same line of thinking is applied to algorithms used to assist in making legal judgments, then the idea of a judge or hearing officer having the final say is rather illusory. It is the algorithm that makes the decision if it is accepted as objective.

While in a classroom setting the blind faith that is placed into software is problematic enough, when framed in a legal context, the opportunity of a fair and impartial hearing is put into question. The opportunity for a fair hearing is a key part of a citizen's due process rights (Citron, 2008; Crawford & Shultz, 2014). In order for there to be a fair hearing process in an algorithmic age, those who have been affected by automated decision-making systems, whether in an administrative law setting or an online environment, are able to make their case and present evidence demonstrating how these systems may have wronged them. Crawford & Shultz (2014) reason that this would include "examining the evidence used, including both the data input and the algorithmic logic applied" (p. 127). The black box nature of algorithms creates difficulties

when attempting to present evidence against any believed algorithmic mis-judgement. As mentioned previously, even if access has been granted to peer inside the black box individuals likely will still not be able to fully understand how to dissect the meaning behind the code.

In the legal world, this inability to possibly understand how automated systems make the decisions they do is one that goes against all fundamentals of law (Hildebrandt, 2009). Not only will policy makers and hearing officers not understand why a computer system gave the output it did, but those who are on the receiving end of the computer assisted determination will also not understand why they are being evaluated in such a way. Subjects of the law have the right to understand the laws that are being placed upon them as part of their due process rights. Citron states that "Laws should be clear and accessible so that those subject to them can know and understand their content" (2008, p. 1297), so when algorithms make the rules inaccessible due process is impossible to achieve since people attempting to appeal a algorithmically derived decision can not even understand why the decision was made in the first place. Crawford and Shultz (2014) point out the Kafkaesque situation algorithms create in the courtroom, where citizens may break rules they were unaware of and when they attempt to learn what rule was broken they are unable to actually discover it. As Kafka himself states in the Trial "It is not necessary to accept everything as true, one must only accept it as necessary" (Kafka, 1999 p. 263**)**

Furthermore, Citron (2008) believes that the potential inadequate notice "will discourage some people from seeking hearings" (p. 1254) in the first place; even if hearings are held it may severely reduce their value. Citron (2008) argues that algorithmic making decision systems jeopardize an individual's legal right to be given notice of an agencies action; "this right requires that notice be reasonably calculated to inform individuals of the government's claims" (p. 1282)

so that a person can prepare themselves for when the action takes effect or to contest the action. Clear notice decreases the likelihood that agency action will rest upon “incorrect or misleading factual premises or on the misapplication of rules” (Citron 2008). Without receiving prior notice of administrative actions being taken individuals have no way to contest any sort of claim made against them. The lack of sufficient notice has become a some what of common occurrence in automated decision-making systems with a number of systems in the United States canceling welfare and Medicaid benefits without notifying individuals before hand. (Citron 2008, Eubanks 2018).

In order to combat the due process issue brought about by the incorporation of algorithms, Citron (2008, 2014), along with Crawford & Shultz (2014) argue that decision making systems should leave behind auditable trails so that law makers and citizens alike can follow the trail of reasoning that guided an algorithm to its conclusion. This audit trail would have to be made legible for non-technical individuals so that due process can be followed. However, while auditable algorithms seem useful in theory, using codes that are then audited to conduct enforcement amplifies problem of magnitude, or "too-much-information," often associated with present day disclosures (Perel & Elkin-Koren, 2017). On top of this, Perel & Elkin-Koren (2017) argue that “it also imposes practical difficulties on relying on transparency as an adequate check for algorithmic enforcement” (p. 1). When it comes to implementing algorithms into legal practices of any sort, transparency is the largest issue, as it is crucial when guaranteeing an individual their due process. This has led much of the legal literature surrounding algorithms fixated on cracking open the black box and exposing the lines of code inside, obviating their decision-making processes. The question remains if this is the best way to

understand the complex socio-technical assemblage of algorithms, especially within morally and ethically entangled legal spaces.

Chapter 3

Case Studies

Transparency, fairness, and the ability to understand how and why legal decisions are made are all necessary facets of an individual's rights to due process. As shown through the literature discussed, algorithms have proven time and time again to be in opposition with these ideals. As mentioned, algorithms are often considered to be black boxes with their coded logic hidden behind IP laws and dense technical language, making calls for true transparency seem like an impossibility. Their increasingly complex nature and opacity makes it difficult for researchers to detect and locate potential implicit biases within the algorithm. While those who make the decisions to use algorithmic systems might view algorithms as objective decision makers, it has become commonly understood among many scholarly circles that they are in fact non-neutral entities.

In order to understand the implications and uses of algorithms within the context of a legal process we will look at two areas of law in which algorithms are currently being used in multiple countries. Firstly, the use of decision-making algorithms in the field of immigration law will be examined to demonstrate the effect that algorithmic decision-making systems have on administrative legal processes. Secondly, the use of algorithms to make risk assessments in bail hearings will be discussed to show that while the algorithms and procedures may differ, much of the same algorithmic challenges arise in criminal law as they do in administrative law. The reason for examining two different field of laws is to show the differences and similarities

between how legal processes, whether administrative or criminal, affect the due process rights of individuals.

Immigration, Algorithms, and Due Process

With immigration becoming more and more of a logistical challenge for governments around the world, as more people attempt to migrate to new countries for any number of reasons, governments are beginning to turn to algorithms as a method to ease administrative backlogs with out breaking the budget. However, marginalized and under-resourced communities such as undocumented individuals, those with temporary status like students, and permanent residents still have their own due process rights, leaving room for algorithms to run a foul and cause harm to an already under resourced communities.For instance, in the United Kingdom a voice recognition algorithm used as part of an English language entrance test for new immigrants, accused tens of thousands of international students of cheating on their TOIEC (Test of English for International Communication) (Sonnad, 2018). Sonnad (2018) explains that "ETS (Educational Testing Service) had tried to identify fraud using voice-recognition software, according to the appeals court decision." Using their voice recognition algorithm, ETS analyzed all the tests from the UK and tried to identify cases where multiple tests had the same voice signature for the oral component. If a voice profile appeared on more than one test it would indicate a fraudulent test as it would mean a single person took the test for multiple people. According to a report published by Migrant Voice (2018):

> with no proper right to challenge the decision, [students] were summarily told that their studies had been terminated and that they had no right to stay in the United Kingdom. Overnight, lives were turned upside down. Some of the students were taken straight to immigration detention, some were deported, and some returned to their home countries to

> appeal against the allegation. Others remained and worked desperately to clear their names, knowing that going home with such a slur hanging over them would have destroyed their reputations and barred them from jobs – and in some cases, destroyed their familial relationships. (p. 5)

ETS's analysis delivered to the Home Office, the department of UK Government that handles immigration and passports, said there were close to 34,000 "invalid" TOEIC test results. On top of that 22,000 further tests were flagged as questionable (Migrant Voice, 2018). While it is noted that voice-recognition software can be vary accurate with a 1% margin of error, it should be noted that even at 1% "several hundred test results marked "invalid" by the technology could have in fact been honest test takers" (Sonnad, 2018). Other errors besides one of algorithmic error could have also occurred, for example some of those who appealed said that the voice recording they were given of their test session was not the correct file (Weale, 2018). According to an immigration lawyer who spoke to *The Guardian*, they place the error rate between 5% and 10%, which would put the number of unjust deportations in the thousands (Weale, 2018).

Migrant Voice's report concluded that the UK Home Office has hindered student's ability to correct any errors made by ETS's software in a number of ways. Firstly, refusing to provide students with evidence critical to their defence in a timely manner (Migrant Voice, 2018). Secondly, relying on evidence that has been highly criticized by the Courts (Migrant Voice, 2018). Lastly, "preventing students from appealing or proceeding with other judicial actions either directly through its decisions or by supporting legislation to take away important appeal rights" (Migrant Voice, 2018).

Unfortunately, the use of decision-making algorithms in the context of immigration is not a unique tool to the United Kingdom. Since at least 2014, Canada has been introducing

automated decision-making elements into its immigration procedures, most notably to automate certain activities currently conducted by immigration officials and to support the evaluation of some immigrant and visitor applications (Molnar, P. & Gill, L., 2018). A report from the Citizen Lab and the International Human Rights Program at the University of Toronto's Faculty of Law investigates the use of artificial intelligence and automated decision-making in Canada's immigration and refugee systems. The report finds that use of automated decision-making technologies "to augment or replace human judgment threatens to violate domestic and international human rights law, with alarming implications for the fundamental human rights of those subjected to these technologies" (Molnar, P. & Gill, L., 2018).

The use of automated decision-making in the sphere of immigration and refugee law and policy is highly problematic and the potential ramifications are far-reaching. Marginalized and under-resourced communities such as undocumented individuals, those with temporary status like students, and permanent residents often have access to less robust human rights protections than those with citizenship and less legal expertise with which to defend those rights. By adopting the use of autonomous decision-making systems without first having an outline of responsible best practices and appropriate human rights principles instilled from the very beginning "may only exacerbate pre-existing disparities and can lead to rights violations including unjust deportation" (Kenyon, M. 2019). According to Citizen Labs, Canada is looking into an expansion of the application of automated decision-making algorithms in a variety of immigration related determinations would normally be made by a human immigration official. The possible decisions that might soon be made by algorithms in relation to immigration and refugee law range in complexity, including whether an application is complete, whether a marriage is genuine, or whether someone should be designated as a risk (Kenyon, M. 2019).

While the idea of an algorithm deciding if a marriage is genuine or not may seem like the plot of a rather dystopian episode of Black Mirror, for future immigrants and refugees it may very well be their reality.

Having the proper tools and methods for auditing algorithms is crucial in providing adequate notice to individuals who lives are being left to the mercy of an automated decision-making algorithm. Not only would auditing allow for individuals to appeal unjust decisions much more effectively after they have been made; it would also allow for the initial decision makers, whether that be immigration officers, administrative tribunals, or judges to make informed decisions in the first place.

Bail, Pre-Trial Risk Assessments, and Transparency

The use of pretrial algorithmic risk assessments in criminal law has expanded rapidly across the United States to the point where these types of systems are "probably the most widely implemented algorithmic tools in use in criminal proceedings in the world" (Law Commission of Ontario, 2020). Algorithmic pretrial risk assessment tools are used to predict how likely it is that an accused is to miss a scheduled court date, potential flight risk, commit another crime, or in more specific cases commit a violent crime. While these types of risk assessment tools may sound like they are ripped right out of a science fiction film like Minority Report or Timecop, where the entire premiss is to sentence people for crimes they have not committed, they are becoming a very real part of the criminal justice system. However, as discussed previously the algorithmic tools in the real world are not objective or neutral because they are based on data (Gitelman, 2013). Data has the potential to be embedded with any number of implicit and explicit biases; "seemingly technical decisions often embed far-reaching policy or legal choices without public discussion or accountability" (Law Commission of Ontario, 2020).

For example, in the 2018 Supreme Court of Canada case of Ewert v. Canada, *"*an Indigenous man argued that the long-standing risk-assessment tools used by the Correctional Services of Canada (CSC) for his parole hearing were unfair because they were tested on non-Indigenous populations" (Hasham, 2019). The court ruled 7-2 in favour of Ewert claiming there is ample reason to doubt the "cross-cultural validity of the CSC's risk tests (measuring recidivism and psychopathy) in their application to Indigenous prisoners" (Beatson, 2018). The risk assessment tools in Ewert v. Canada case were not machine learning, in that the algorithm did not update or change its parameters by itself based on the calculations made automatically by the algorithm. Machine learning algorithms are more impenetrable and complex when it comes to understanding why decisions are made as stated previously, so the fact that CSC's risk tool lacked machine learning abilities and was found unfit to make judgements based on race only shows the problems that could be obfuscated by using automated decision-making systems in the legal process.

The potential for implicit racial bias in algorithmic systems used in legal decision-making processes has been well documented (Angwin et al., 2016; Molnar, P. & Gill, L., 2018) and perhaps there is no better example than the investigation into Northpointe, Inc.'s algorithmic recidivism tool, called COMPAS (which stands for Correctional Offender Management Profiling for Alternative Sanctions). The COMPAS algorithm is one of the most popular scores used in the United States and is increasingly being used in pretrial and sentencing, which is why it was chosen for analysis (Larson et al. 2016). An investigation conducted by ProPublica found that "black defendants were far more likely than white defendants to be incorrectly judged to be at a higher risk of recidivism, while white defendants were more likely than black defendants to be incorrectly flagged as low risk" (Larson et al, 2016). Black defendants were often predicted to

be at a higher risk of recidivism than they were in reality. The analysis found that black defendants who did not re-offend over a two-year period were nearly twice as likely to be misclassified as higher risk compared to their white counterparts (45 percent vs. 23 percent) (Angwin et al. 2016). On the other hand, white defendants were often predicted to be less risky than they actually were, as the analysis found that white defendants who re-offended within the next two years were mistakenly labeled low risk almost twice as often as black re-offenders (48 percent vs. 28 percent) (Angwin et al. 2016).

The COMPAS risk assessment tool was not only used to predict general recidivism but was also said to be capable of predicting a defendant's risk of committing violent crime if released on bail (Angwin et al. 2016). And just like the racial bias found within the recidivism algorithm just mentioned, the algorithm used to judge whether or not a defendant was likely of specifically violent recidivism was also skewed to be prejudice of black defendants. Larson et al. found that "Black defendants were twice as likely as white defendants to be misclassified as being a higher risk of violent recidivism. While white violent recidivists were 63 percent more likely to have been misclassified as a low risk of violent recidivism, compared with black violent recidivists" (2016). The fact that any algorithm claims to be able to accurately predict the risk of pretrial violence is almost inherently flawed. Pretrial violence is exceedingly rare, which makes it challenging to statistically predict as there is likely not enough data to create a model accurate enough to make a prediction that could be held to the high standards of the law (Barabas et al. 2019). Barabas et al. plainly state that

> Risk assessments cannot identify people who are more likely than not to commit a violent crime. The fact is, the vast majority of even the highest risk individuals will not go on to be arrested for a violent crime while awaiting trial. Consider the dataset used to build the

> Public Safety Assessment (PSA): 92% of the people who were flagged for pretrial violence did not get arrested for a violent crime and 98% of the people who were not flagged did not get arrested for a violent crime. If these tools were calibrated to be as accurate as possible, then they would predict that every person was unlikely to commit a violent crime while on pretrial release. (2019).

Ultimately, these types of risk assessments could easily lead judges to overestimate the risk of pretrial violence and cause more people to be locked up before trail than is actually necessary. A recent study found that people tend to significantly overestimate the recidivism rate for individuals who are assessed as moderate to high-risk by the kinds of risk assessment tools discussed in this section. (Daniel et al. 2018) Participants of the study greatly overestimated the actual rate of recidivism for those assessed as moderate to high-risk category, “the true rate was less than fifty percent of what participants predicted” (Daniel et al. 2018). The easy solution some might say would be to simply exclude race as a variable that the algorithm considered when it formulates a decision. However, excluding race itself does not necessary mean that factors that serve as proxies to an individual’s race are excluded from these algorithms. An example of a factor that correlates heavily with an individual’s race could be the number of times they have been stopped by the police. As data scientist Cathy O’Neil writes her book, Weapons of Math Destruction:

> [I]t’s easy to imagine how inmates from a privileged background would answer one way and those from tough inner-city streets another. Ask a criminal who grew up in comfortable suburbs about “the first time you were ever involved with the police,” and he might not have a single incident to report other than the one that brought him to prison. Young black males, by contrast, are likely to have been stopped by police dozen\s of

> times, even when they've done nothing wrong… So if early "involvement" with the police signals recidivism, poor people and racial minorities look far riskier. (O'Neil, 2017. p 18)

The COMPAS algorithm like many automated decision-making algorithms used in legal decision making is proprietary and owned by Northpointe, a consulting and research firm that delivers software products, training, decision support and implementation services. The technologies and their inner workings are closely guarded secrets of the companies that create them. As previously mentioned, if the code that makes up the logic and procedural functioning of the algorithm are exposed the system can be gamed by individuals, or the code could be replicated diminishing any value the original may have had. The potential of "gaming" a pre-trial risk assessment would completely invalidate the tool and make a farce out of the hearing itself. However, without being able to fully understand how an algorithm comes to make its decisions, defendants are left with an asymmetry of knowledge that places them at the mercy of a seemingly rigid and opaque system, one that infringes on their right to due process. Hildebrandt incisively states "There is no business model for effective transparency tools, through there certainly is a business model for tools that merely simulate transparency. Real transparency would threaten the monetization of data, disabling the profitability of pre-emption itself" (2015, p.102)

The rules stitched into the social fabric of society by search engines, are partly written by coders, engineers, and computer scientists responsible for the coded lines that make up the algorithms, as mentioned by Noble (2018) and Pasquale (2006). While they are not entirely responsible for the actual use of their software by their clients, they are responsible for many of the rules that underline how an algorithm function. When this understanding is placed within a

legal framework those responsible for coding algorithms that make decisions affecting people civil liberties, the computer programmers and engineers can be seen as rewriting the law (Hildebrandt, 2009). When programmers are tasked with writing an algorithm to be used in a legal setting, they are interpreting the rules, laws, and legislation that has been put in place so that it can be translated into a computer interface (Hildebrandt, 2009). Code writers are not policy experts and may not always fully understand, or may misinterpret, what they are programming into an automated system, not to mention the possible effects that this reinterpretation may have on individuals subjected to the decision-making system. When it comes to decerning between a code choice and a policy choice it is sometimes difficult to appreciate the difference (Law Commission of Ontario, 2020). These reinterpretations of the law effectively, while seemingly unintentionally, usurp a decision maker's, (such as a judge, hearing officer, or committee) own expertise and authority on whatever legal decision they may preside over. By bypassing the expertise of policy makers, hearing officers and judges, algorithmic decision-making systems are becoming both the rule maker and adjudicator in society. This dual role that algorithms are beginning to play in the legal systems of North American has Hildebrandt arguing that if we do "not embody legal norms in new technological devices and infrastructures, we may reach the end of law" (2009).

Claims of the "end of law," however, are by no means purely hyperbolic. Citron (2008, 2014), Pasqual (2006), and Crawford & Shultz (2014), all agree with Hildebrandt, that the fundamental underpinnings of the law, fairness, transparency, and accountability, are jeopardized by the use of algorithmic systems; they all agree that there is one crucially important facet of their use that must be addressed in order to avoid law's demise: transparency. Due process frameworks outline the need for the opportunity of a fair hearing, where those who have been

affected by automated decision-making systems, whether in an administrative law setting or an online environment, are able to make their case and present evidence demonstrating how these systems may have wronged them. Crawford & Shultz reason that this would include "examining the evidence used, including both the data input and the algorithmic logic applied" (2014). One significant way to do this in any meaningful capacity would be to develop a method of auditing the algorithms so that both decision-makers and those who are on the receiving end of algorithmic judgments are able to examine just how and why the algorithm came to the conclusions it did.

Chapter 4

Auditing Decision-Making Algorithms

With the growth in the study of algorithms over the last 10 years there have been many meaningful suggestions on how best to tackle the issues surrounding the topic of algorithmic transparency. As previously mentioned, some researchers primarily in the communications and science and technology studies (STS) fields believe that true transparency might be somewhat of a fallacy and that what should be strived for is a way of unknowing algorithms as discussed in Chapter 3. That is, to recognize their inherent opacity and work with those limitations rather than focusing too much energy on opening the algorithmic black box, essentially focusing on the inputs and outputs rather than the impenetrably complex source code (Butcher, 2018. p.46). Others have suggested that attempting to reverse engineer an algorithm for study might be the best course of action for researching some types of algorithms (Diakopoulos, 2013). Some have suggested not focusing on the algorithm itself, but rather conducting ethnographies of the coding and interviewing the developers (Kitchin, 2016).

While each of these research methods have their merits and can be effective for studying web algorithms that people encounter during their everyday lives, such as Google search algorithms (Noble, 2018) or YouTubes recommendation algorithms (Lewis & McCormick, 2018), when it comes to decision-making algorithms that operate within a criminal or administrative law setting, where individuals are expected to receive due process rights, these methodologies may not be quite as useful. While this is not to say that these research methods are not capable of providing insight into algorithms like the ones mentioned in the previous case studies; any analysis of these algorithms using these methods would come after a decision has been made thus still allowing for due process rights to be violated. What I propose, based on the material discussed in this MRP, to be the most effective solution for both studying algorithms that are used for legal decision-making processes and preserving an individual's right to due process is conducting an audit study of the algorithm in question.

While the term audit is normally associated with the financial industry, audit studies are somewhat different from the common understanding of the term. Audit studies are typically field experiments in which researchers participate in a social process that they suspect to be corrupt in order to determine if there is any discrimination taking place. In fact, "the original audit studies were developed by government economists to detect racial discrimination in housing by the research unit of the US Department of Housing and Urban Development in the 1970s" (Sandvig et al, 2014). Christian Sandvig, a communications scholar who studies algorithms and their potential for bias has outlined several ways in which the concept of an audit study can be designed to, "investigate normatively significant instances of discrimination involving computer algorithms operated by Internet platforms" (2014). While Sandvig et al's proposed research design is focused on the algorithms encountered on the internet on a day-to-day basis I believe

that some of them can be useful in auditing decision-making algorithms that are used in legal processes. Audit studies, because of their legal context, are by design meant to be simple enough that a lawyer or judge can understand them and use them as evidence in court case. While Sandvig et al proposes five possible audit types for studying internet algorithms, I believe only two would be useful in the effort to preserve due process rights when algorithms are utilized in a law setting: a Code Audit (Algorithm Transparency) and a Scraping Audit. Both audit types will be examined in order to demonstrate the strengths and weakness of each method when it comes to preserving the two key facets of due process that have been established earlier: the right to adequate notice and the right to a fair hearing.

Code Audit (Algorithm Transparency)

The first type of audit study proposed is a code audit. A code audit is exactly as it sounds, an audit of the actual computer code where researchers can scrutinize the logical foundations of the algorithm. This process should be mandatory for any private company or government institution wishing to use their algorithmic tools with the context of a legal decision-making process to prevent the types of algorithmic misbehavior discussed throughout this MRP. Code should have to be released to an independent, government-appointed third party for inspection to observe and algorithmic misbehavior before it is implemented into any legal procedure. Unfortunately, today private companies consider their algorithms to be valuable intellectual property and aim to shadow their inner workings behind trade secret protection laws. (Pasquale 2010; 2011). Private corporations are unlikely to hand over the code to their algorithms (especially illegal algorithms) unless the disclosure of said algorithm were to be compelled as necessary for them to have their product used by a governing body. There is a crucial problem to this method of auditing, since an algorithm is essentially a formula that when given a specific set

of variables produces a particular result, there is room for them to be manipulated if their code is made public. In the legal context, if both parties (decision maker and receiver) are given access to the code and presuming they have the necessary knowledge, they could game the algorithm produce an output that is more favorable of their argument. For example, in the case of immigration, if hopeful immigrants knew what data an algorithm used to make a decision and the logic behind why the decision was made, they could omit or fabricate information that the algorithm viewed as favorable to their case.

While the potential for gaming an algorithm that is used to provide fair and impartial judgements may make this audit method seem impractical, there are possible solutions, such as making much of the code available for review while hiding only selective bits of code. By using open-source internet platforms that make their algorithms available to the public as an example, websites such as Reddit, who allow their code to be examined, scrutinized, and re-purposed all while operating a highly successful platform are able to do so by keeping parts of their code secret. To prevent spambots from using the disclosed algorithm to manipulate the users experience while visiting Reddit, “a kernel of the algorithm (called the “vote fuzzing” code) must remain closed source and secret, despite Reddit’s aspirations to transparency” (Sandvig et al, 2014). While adopting this “semi-transparent code” strategy into an algorithm used with in the context of law is not ideal as anything less than true transparency is likely to create calls for due process right violations, it is a least a step in proving greater transparency than what is currently available to decision-makers and decision-receivers.

Pasquale (2010) has proposed an alternative solution to this problem wherein algorithms themselves could be disclosed to third party specialists who would keep them private while still permitting public interest scrutiny, but not allowing for the algorithms to be fully disclosed to the

public. If Pasquale's proposal were to be implemented, it would dramatically improve this research design. Even if organizations expected their algorithms to be audited, they may not know exactly what details the auditors are looking for, making it difficult for them to try and hide any algorithmic misconduct.

Even with these proposed solutions to the transparency problem of this audit study method there are still limitations. Even at the normal level of complexity at which decision-making systems operate an algorithm cannot be interpreted solely by reading it. Meaning scrutineers of a specific algorithm are not going to find a line like:

"if ($race = NOT_CAUCASIAN) then { illegal_discrimination() };" (Sandvig, et al., 2014).

As mentioned previously, algorithms are more than the lines of computer code, they are best understood as a technical assemblage. An algorithm is useless without information; depending on the information that is fed into the algorithm the resulting output can vary widely. Depending on the data set used an algorithm that appears to be completely free of any sort of bias while using one set of information can begin perpetuating harmful recommendations, predictions, or judgements. As was the case The Ewert v. Canada example discussed previously, if the data set that the algorithm uses to make decisions is tainted with bias, then the algorithm is likely to produce results that perpetuate that same bias. While the code audit might be useful in some situations or as an auxiliary tool, it is important to consider alternative research designs for algorithm audits that might address the limitations of performing just code audits.

Scraping Audit

In a scraping audit, rather than using the code itself as the point of examination the fixation is on the inputs and outputs of the algorithm in question. Researchers would be given access to the algorithm to run different experiments where they would repeatedly give the algorithm information in order to observe the results of its processes. In doing so researchers would be able to discover potential patterns that the algorithm has in its decision-making process; if a pattern were to be discovered where researchers notice the algorithm was giving biased results, they would be able to report it, locate the flawed code logic, correct it, and start the process again to see if the changes create any new issues. By meticulously testing the inputs and outputs to see what inputs generate what outputs researchers would be able to document any potential patterns that begin to arise. The reason this method is term a scraping audit is because it typically involves running software on a website that would rapidly generate an input, then document the output a long with any possible web code that it code find in order to reverse engineer the way the algorithm came to that conclusion (Sandvig et al, 2014). If researchers where given access to test judicial algorithms using software that could scrape data in a similar manner, many insights into the decision-making patterns of an algorithm could be learned. This would help to provide transparency, understandability, and fairness for both decision-makers and receivers in legal systems.

This method of dissecting an algorithm’s inputs and outputs is a common practice among web researchers. This method was used by *The Atlantic* when it discovered Netflix’s 76,897 algorithmically generated micro-genres of movies (Madrigal, 2014). This was accomplished by copying and pasting URL codes into the address bar and seeing what genres come up. The researcher had learned that Netflix's genre URLs were sequentially numbered. Realizing that

"one could pull up more and more genres by simply changing the number at the end of the web address" (Madrigal, 2014). By playing with the input (URL code) and documenting the output (genre recommendation) the researchers were able to gain insights in to not only the number of different genres Netflix has, but more interestingly the grammar Netflix uses to create new genres.

This method of reverse-engineering an algorithm is a much easier task when attempting to understand publicly accessible algorithms like Netflix recommendations, however when it comes to tinkering with the inputs and outputs of a risk assessment algorithm used in bail hearings access is essentially impossible. As mentioned previously the algorithms used are often intellectual property belonging to private companies constituting a trade secret. If the algorithm is produced by a government organization, examining its ins and outs is still a point of concern, due to possible "gaming" of the system to avoid being flagged by the algorithm in situations that should be, as shown in the immigration example mentioned previously. To get around these hurdles the best solution would be for the government to set up an independent oversight group where the algorithms in question can be tested extensively by researchers to make sure they are operating and using data in a way that upholds an individual right to due process.

This method of scrape auditing has been used before in a legal context, specifically in the realm of copyright law. Researchers Perel & Elkin-Koren (2017) wanted to examine how YouTubes algorithm enforced copyright takedown notices and flagged illegal content. While the researchers were able to learn about YouTubes processes by uploading copyrighted content and documenting the outcome, they did note that much of what they were doing violated the US Computer Fraud and Abuse Act (CFAA). For instance, to test how YouTubes algorithm handled copyright claims that would have to knowingly upload copyrighted material. Or if they wanted to

test YouTubes ability to flag illicit content, they would have to knowingly upload content that may in fact be illegal.

Whether it be tinkering with inputs and outputs or scraping the code of the algorithm that is available, the process is often deemed as breaching the rights of the algorithm's owner. The CFAA has been criticized as "overbroad legislation that criminalizes unauthorized access to any computer" (Sandvig et al, 2014) and where authorization can be defined by the algorithm's operator. While this would make it difficult for independent researchers to examine an algorithm, if a government committee oversaw researching the decision-making algorithms like the ones used in immigration processes or bail hearings the laws similar to the CFAA would likely be less of a concern. It is clear that researchers are able to learn valuable information about the decision-making processes of algorithms by experimenting with the inputs and outputs, essentially learning how the algorithm thinks. If researchers or government auditors were given access to both an algorithm's code and the freedom to tinker with the algorithm itself, providing transparency to individuals who are receiving algorithmic judgments would be a much more achievable. If meaningful transparency can be achieved where all parties involved in the legal process, from judge or tribunal to defendant or applicant, then the due process rights of an individual can be upheld.

Conclusion

With use of algorithms now moving into the courtrooms and making decisions that directly affect the lives of those who are on the receiving end of such decisions, the need for a comparative look at the research on algorithms is pressing. Legal processes do not happen in a vacuum and the decisions made within these governing systems affect how society and those in it structure and compose reality. While the inclusion of algorithms in legal processes may be

done to improve efficiency of the system, any benefits they may add to the process must be weighed against the negatives, and algorithms are far from error free entities. Algorithms are black boxes in nature, with their processes itself shielded from scrutiny from those on the outside. The black box nature of algorithms is paradoxical to the transparency required in a just legal system and thus requires extensive research. This MRP has discussed several ways in which algorithms negatively impact an individual's due process rights, from their lack of transparency and potential for bias, to their ability to make and implement decisions before individuals have the chance to appeal any claims. While solutions to these problems can be complex this MRP offers what I think are steps in the right direction for better protecting an individual's due process rights when algorithmic tools are used for judicial purposes. By using code audits and scraping audits, along with independent government oversite groups, upholding due process rights despite the use of algorithms can be an achievable goal.

Rather than regulating for transparency or misbehaviour of algorithms used in legal processes this MRP argues for a regulation towards the auditability of algorithms. Transparency does not always mean understandability as shown when it comes to disclosing an algorithms code. Without understanding there can be no effective right to due process. Regulating for auditability requires a third-party role for governments and researchers, to hold algorithmic systems accountable by auditing them before their implementation within a given legal process, as well as repeatedly after they have been implemented. As noted by Sadvig (2014) "this would require financial and institutional resources that would support such an intervention," which means that a sort of algorithm accountability committee will need to be formed for the public interest. This kind of oversight committee may also be welcomed by a wide range of stakeholders, such as the ones discussed by Sandvig et al (2014) who are interested in auditing

web-based algorithms like ones used by Facebook and Google. If having to explain how an algorithm came to its conclusion, is too much of a burden then these systems should not be in use. If an algorithm decides that a person is no longer eligible to receive medical benefits or finical assistance the administrative procedures should clearly explain how and why the algorithm made its decision. If a person is deported because an algorithm says they cheated on the language test, then they should be able to challenge that decision and understand why the algorithm came its conclusion. And if a person accused of a crime is told they will not be allowed the opportunity to make bail because they are perceived to be at a high risk for recidivism, then the burden should be on the court to show why the algorithm came to that conclusion before taking the accused freedoms away.

References

Angwin, J., Larson, J., Kirchner, L., & Mattu, S. (2016). Machine bias https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal sentencing

Angwin, J., Mattu, S., Larson, J. (2015, September 1). The tiger mom tax: Asians are nearly twice as likely to get a higher price from Princeton Review. ProPublica. https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from princetonreview#:~:text=Asians%20More%20Likely%20To%20Be,for%20its%20SAT% 20prep%20packages.

Baker, P & Potts, A. (2013). Why do white people have thin lips?, google and the perpetuation of stereotypes via auto-complete search forms." *Critical Discourse Studies* 10(2): 187-204.

Barabas, C. et al. (2019). Technical flaws of pretrial risk-assessments raise grave concerns. MIT Media Lab. https://dam-prod.media.mit.edu/x/2019/07/16/TechnicalFlawsOfPretrial_ML%20site.pdf

Beatson, J. (2018). Ewert v Canada: Improving prison processes for indigenous peoples? The Court. http://www.thecourt.ca/ewert-v-canada-improving-prison-processes-for-indigenous-peoples/

Beer, D. (2009) Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media and Society*, 11(6), 985-1002.

Benner, K., Thrush, G., & Isaac, M. (2019). Facebook engages in housing discrimination with its ad practices, U.S. says. New York Times. https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html

Bucher, T. (2012). The friendship assemblage: Investigating programed sociality on Facebook. *Television & New Media,* 14(6), 479-493.

Bucher, T. (2018). *If .... then: Algorithmic power and politics*. New York, NY: Oxford University Press.

Carty, S. (2011). Many cars tone deaf to women's voices. Autoblog, May 31. http://www.autoblog.com/2011/05/31/women-voice-command-systems/.

Cheney-Lippold, J. (2011). A new algorithmic Identity: Soft biopolitics and the modulation of control *Theory, Culture & Society, 28*(6), 164-181

Citron, K. (2008). Technological due process. *Washington University Law Review*, 85(12), 49-1313.

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

Crawford, K., Jason, S. 2014. Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review,* 55(1): 93+.

Daniel A., Krauss, Gabriel I. Cook & Lukas Klapatch, 2018. Risk assessment communication

difficulties: An empirical examination of the effects of categorical versus probabilistic risk communication in sexually violent predator decisions, *Behavioural Science & the Law, 35(5): 532-553.*

Datta, A., Tschantz, M. C., & Datta, A. (2015). Automated experiments on ad privacy settings. *Proceedings on Privacy Enhancing Technologies*, (1), 92–112.

Diakopoulos, N. (2013). What words do Bing and Google ban from autocomplete? http://www.slate.com/articles/technology/future_tense/2013/08/words_banned_from_bing_and_google_s_autocomplete_algorithms.html

Diakopoulos, N. (2015). "Algorithmic accountability." *Digital Journalism*, 3(3): 398–415.

Dijck, J. V. (2013). *The culture of connectivity: A critical history of social media*. New York: Oxford University Press.

Eubanks, V. (2017). Automating inequality: How high-tech tools profile, police, and punish the poor. Picador.

Ferguson, A. G. (2017). *Rise of big data policing: Surveillance, race, and the future of law enforcement*. New York University Press.

Friedman, B & Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems.* 14(3), 330-347.

Foucault, M. (1977). *Discipline and punish: The birth of the prison.* New York,: NY Vintage.

Foucault, M. (2003) Society Must Be Defended: Lectures at the Collège de France, 1975–

1976. New York: Picador.

Foucault, M. (2008) The Birth of Biopolitics: Lectures at the Collège de France, 1978–1979. New York: Palgrave Macmillan.

Gillespie, T. (2016). Algorithm, in *Digital keywords: A Vocabulary of information society and culture*, edited by Ben Peters. Princeton: Princeton University Press

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

Grimmelmann, J. (2005). Regulation by software. *The Yale Law Journal, 114*(7), 1719-1758.

Hasham, A. (2019, July 19). *Soon, intelligent machines could help decide whether to keep people in jail. it's time to prepare*. Toronto Star. https://www.thestar.com/news/gta/2019/07/19/soon-intelligent-machines-could-help-decide-whether-to-keep-people-in-jail-its-time-to-prepare.html.

Hildebrandt, M. (2009) Technology and the end of law. In: Keirsbilck B., Devroe W., Claes E. (eds) *Facing the limits of the law* (pp. 443-464). Springer, Berlin, Heidelberg.

Hildebrandt, M. (2016). *Smart technologies and the end(s) of law: novel entanglements of law and technology*. Edward Elgar Publishing.

Introna, L. (2004). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance & Society,* 2(2), 177-98.

Introna, L. (2016). Algorithms, governance, and governmentality: On governing academic

writing. *Science, Technology, & Human Values, 41*(1), 17-49.

Joerges, B. (1999). Do Politics Have Artefacts? Social Studies of Science, 29(3), 411–431.

Kafka, F. (1999). *The Trial*. Schocken Books.

Kehl, D. Guo, P., and Kessler, S. 2017. Algorithms in the criminal justice system: Assessing the use of risk assessments in sentencing. Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School.

Kenyon, M. (2019, April 10). Bots at the Gate: A human rights analysis of automated decision making in Canada's immigration and refugee system. https://citizenlab.ca/2018/09/bots-at-the-gate-human-rights-analysis-automated-decision-making-in-canadas-immigration-refugee-system/.

Kitchin, R. (2016). Thinking critically about and researching algorithms. *Information, Communication & Society*, 20 (1), 14-29.

Larson, J. et al. (2016, May 23). How we analyzed the COMPAS recidivism algorithm. ProPublica. https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

Law Commission of Ontario (2020), The Rise and Fall of AI and Algorithms In American Criminal Justice: Lessons for Canada.https://www.lco-cdo.org/wp-content/uploads/2020/10/Criminal-AI-Paper-Final-Oct-28-2020.pdf

Lewis, P., & McCormick, E. (2018, February 02). How an ex-YouTube insider investigated its

secret algorithm. *The Guardian.*

https://www.theguardian.com/technology/2018/feb/02/youtube-algorithm-election-clinton-trump-guillaume-chaslot

Lyon, D. (1998). The world wide web of surveillance: The internet and off-world power-flows. *Information, Communication & Society*, 1(1), 91-105.

MacAskill, E., & Dance, G. (2013, November 1). NSA files decoded: Edward Snowden's surveillance revelations explained. The Guardian.

https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/2.

Madrigal, A. (2014). How Netflix reverse-engineered hollywood. The Atlantic.

https://www.theatlantic.com/technology/archive/2014/01/how-netflix-reverse-engineered-hollywood/282679/.

Migrant Voice. (2018). *I want my future back: The international students treated as guilty until proven innocent.* Migrant Voice.

https://www.migrantvoice.org/img/upload/I_want_my_future_back_report.pdf

Molnar, P. & Gill, L. (2018). Bots at the gate: A human rights analysis of automated decision-making in canada's immigration and refugee system. Toronto: University of Toronto International Human Rights Program (IHRP) at the Faculty of Law and the Citizen Lab at the Munk School of Global Affairs and Public Policy. Retrieved From

https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report Web-V2.pdf

Murphy, M. (2017). Algorithmic surveillance: The collection conundrum. *International Review of Law, Computers & Technology*, 31(2), 225-242.

Noble, Safiya. (2012). Missed connections: What search engines say about women. *Bitch magazine*, 12(4): 37-41.

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

O'Neil, C. (2017). *Weapons of math destruction: how big data increases inequality and threatens democracy*. Penguin Books.

Pasquale, F. 2006. Rankings, reductionism, and responsibility. *Cleveland State Law Review*, 54, 115-139.

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

Perel, M.; Elkin-Koren, N. (2017). Black box tinkering: Beyond disclosure in algorithmic enforcement. *Florida Law Review* 69(1), 181-222.

Sandvig, J., Hamilton, K ., Karahalios, K., Langbort, C. (2014) Auditing algorithms: Research methods for detecting discrimination on

internet platforms. International Communication Association. May 22, 2014; Seattle, WA, USA. http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20--%20Sandvig%20--%20ICA%202014%20Data%20and%20Discrimination%20Preconference.pdf

Sonnad, N. (2018). A flawed algorithm led the UK to deport thousands of students. Quartz. https://qz.com/1268231/a-toeic-test-led-the-uk-to-deport-thousands-of-students/

Srnicek, N. (2017). *Platform capitalism*. Cambridge: Polity.

Tatman, R. (2016). Google's speech recognition has a gender bias. Making Noise and Hearing Things. Retrieved from https://makingnoiseandhearingthings.com/2016/07/12/googles-speech-recognition-has-a-gender-bias/.

Vincent, J. (2016). Twitter taught Microsoft's friendly AI chatbot to be a racist asshole in less than a day. The Verge. Retrieved from https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist

Weale, S. (2018, May 1). Sajid Javid warned over students forced from UK after language tests. The Guardian. http://www.theguardian.com/politics/2018/may/01/sajid-javid-urged-to-review-plight-of-students-forced-out-of-uk

Willson, M. (2016). Algorithms (and the) everyday. *Information, Communication & Society*, 20 (1), 137-150.

Winner, L. (1980). Do artifacts have politics? *Daedalus*, *109*(1), 121-136.

Ziewitz, M. (2016). Governing algorithms: Myth, mess, and methods. *Science, Technology, &*

Human Values, 41(1), 3-16.

Vita Auctoris

Paul Baillargeon was born in 1991 in Windsor, Ontario. He graduated from St. Anne's High School in 2009. From there he went on to Fanshawe College where he obtained a diploma in Music Industry Arts in 2011 and a post-graduate certificate in Audio Post-Production in 2012. Following his time at Fanshawe, he went on to the University of Windsor where he obtained a B.A. (Hons) in Communication, Media & Film in 2018. He is currently a candidate for the Master's degree in Communication and Social Justice at the University of Windsor and hopes to graduate in Summer of 2021.