Taming the Leviathan: How Algorithmic Regulation Alters the Relationship Between Government and Constituent

Kaley Nicole Cook

Student Number: 59680

Roskilde University

MA Thesis

Global Studies and Cultural Encounters

Spring Semester 2018

1 June 2018

Supervisor: Johan Fischer

Character Count: 147,231

Contents

Abbreviations

ACLU – American Civil Liberties Union

CPD – Chicago Police Department

DCFS – Department of Children and Family Services

EU – European Union

GDPR – General Data Protection Regulation

NYPD – New York Police Department

NYT – New York Times

RSF – Rapid Safety Feedback

SSL – Strategic Subject List

US – United States

Abstract

This thesis a theoretical study of the relationship between government, technology, and constituents, focusing on algorithmic regulation and modern American governance. Taking point of departure in the governmental philosophies of Giorgio Agamben and Michel Foucault and engaging with the concept of 'anticipatory governance,' the study utilizes two case studies from Chicago, Illinois and the application of the Strategic Subject List and the Rapid Safety Feedback. The cases are analyzed with the use of four main themes of security, privacy, efficiency, and effectivity and then combined with the philosophies of Agamben and Foucault, resulting in the establish of the shifting role of the government toward anticipatory governance and the subsequent call for a response that also anticipates future problems and calls for greater regulation of algorithmic regulation going forward.

Dette speciale er et teoretisk undersøgelse, som gennemgår forholdet mellem regering, teknologi og borger, med et sær fokus algoritmisk regulering og moderne Amerikansk regeringsføring. Opgaven tager som udgangspunkt statslige filosofier af Giorgio Agamben and Michel Foucault og engagering af konceptet 'anticipatory governance,', hvor derefter to cases fra Chicago bliver analyseret, nemlig anvendelsen af 'Strategic Subject List' og 'Rapid Safety Feedback'. De to cases bliver analyseret i forbindelse med primær temaer såsom sikkerhed, privatliv og effektivitet, hvor derefter bliver kombineret med Agamben og Foucault's filosofier. Resultatet førte til etableringen

Keywords: algorithmic regulation, predictive analytics, technology, governance, Agamben, Foucault, regulation, America

1. Introduction

1.1. Background and Formulation

In 1999, television writer Aaron Sorkin and his freshman network juggernaut, *The West Wing*, brought a seemingly banal debate into primetime. On the critically acclaimed show, known for its superstar cast and its exploration of life within the White House through dramatic storylines ranging from terrorism to diplomacy, the characters performed their famous 'walk and talks' about a new subject: the United States' census. In the episode, West Wing staffers, portrayed by Rob Lowe and Richard Schiff, are tasked with preparing for a partisan debate on the collection of census data and its socio-political implications. Central to the political debate is a new algorithm – a strand of instructions for calculation that makes computing possible – that could collect the data faster, cheaper, and more accurately than the incumbent method of door-to-door collection. This traditional method, the audience is told through the dialogue, is not only inordinately expensive but is also biased in its task of counting those who are residing in America – "over-representing white, middle-to-upper class Americans and under-representing minorities and the homeless" (Cook, 2017, p. 1). The new algorithm proposed could generate more accurate statistics, based on a computer program instead of a national door-to-door data collection campaign. It is argued that the use of the would correct this imbalance, provide a more accurate representation of America, and "count those that needed to be counted the most" (Sorkin, 1999).

In the story, the fictional White House staffers were convinced that the technology proposed would provide not only economic benefits for the government – and, subsequently, the tax payers – but social benefits for minorities as well, providing a method of making a fairer nation for all those that live within the country. The oppositional members of Congress believed the new technology represented a threat to the US Constitution and the democracy it represents by exchanging a task previously completed by humans and replacing it with, essentially, instruction for a math equation. An algorithm, they argued, was no replacement for a human being, especially when the job in question had been designed to be completed by one in an important governmental document.

Within the episode, Sorkin offers no further explanation of the actual mechanics of this fictional algorithm – nor did he need to do so. At its heart, the episode is "not about whether or not the algorithm works, but whether or not it *should*" (Cook, 2017, p. 1), engaging not with the specific mechanics behind its use in the census data collection, but instead with the broader conception of the role of government in the face of new technology. This issue remains pertinent today, with new technology advances coupling with governance more and more in recent years (Guston, 2014). The use of technology affects how governments work with other governments, how they work within themselves, and, of course, how they work with their constituents. This changing way global politics – both internationally and domestically – utilizes technology to interact with citizens is a crucial new frontier for Global Studies. In global politics, as technology increases, it is critical to understand how technology affects governance and how it affects the citizens to which it is applied.

Taking a point of departure in governmental theory, this thesis seeks to explore the relationship between governance and technology through an analysis of algorithmic regulation in the United States of America and the varying levels of success achieved through the application of algorithmic-based programs by state governments. These programs are ubiquitous across the country but can face very little regulation of their own, generating both strong support and criticism for their usage on both a state and federal level in the US. The state of Illinois and its capital, Chicago, have an inconsistent history with the use of algorithmic regulation, especially when used in predictive analytics – a specific form of algorithmic regulation that utilizes identifiers and patterns to generate the statistical probability of a future event. The state has utilized algorithm-driven predictive analytics to attempt to identify participants in gun violence and child abuse, with differing levels of success. Illinois is not the only state to rely on algorithm-produced data for governance either. Due to the unique assets offered by the technology, including opportunities for a response to criminal and social issues that were previously unavailable, any controversies around them have been unable to quell their spread. While their use offers many potential benefits, however, the existence of these programs and their use within a democracy must be considered more carefully. To do this, the role of government itself must be questioned and evaluated alongside these programs to see how their usage affects governance, the costs – social, political, and economic – of their implementation within society, and how it reflects the political trends of the era.

Seventeen years ago, Sorkin and his characters were engaging with an idea that would not be given a name until technology writer and "ideas man" Tim O'Reilly coined the term 'algorithmic regulation' in 2011 (Morozov, 2014). 'Algorithmic regulation' is a broad term that can encompass all manner of governance and law enforcement that are reliant upon the performance of algorithms. The scope of algorithms is modern society is massive, including all forms of automation such as search engines, computers, and numerous other programs that can replace jobs formerly performed by governmental personnel or accomplish new tasks beyond the capabilities of any personnel (Morozov, 2014). The prevalence of algorithmic regulation has greatly increased in the past few decades – with varying degrees of success, societal acceptance, or even public awareness.

Coming to the forefront of societal discussion and academic study in the past few years, algorithmic regulation has become a central controversy in the debate on the relationship between government and technology. It raises numerous questions: How much technology should the government be using? How can a government contend with an increasingly technological society? How do algorithmic regulations work in a democratic society? These questions strike at the role of democratic government itself – and how much of it can reasonably be managed by a math equation.

The debate surrounding algorithmic regulation plays into the larger debate about global politics: the role of government today – and how the role has changed since its initial conception thousands of years ago. With a history better measured in millennia than centuries, new technology certainly requires an updated understanding of governmental theory. Even the US Constitution – not even three centuries old – has been facing criticism over the Second Amendment, "the right to bear arms", and its usage in a modern world with newer weaponry and an increased firepower likely unimaginable by the writers of the Constitution (US National Archives, 2018). Certainly, the same argument could be applied to government and technology on a broader, global scale. No thread of Greek philosophy, nor any historical revolution, can fully contend with the relationship between the modern-day level of technology and governance. In many ways, it is uncharted political territory.

This is not to say that technology does not have a history. Even though it lacked its modern name, algorithmic regulation has been around for decades (Morozov, 2014). But its increased

visibility in the past few years has brought about new praises and critiques regarding its role in governance – especially in democratic governments. If, at least theoretically, the power in a liberal democracy lies with the people, where does the power of algorithms fit in? If current governmental theory was designed to be run solely by humans, how does it evolve with changes in technology that include algorithmic regulation? The triad of liberal democratic governments, their constituents, and algorithmic regulation poses these questions about the role of governments today and the potential dangers. While the benefits of a census-taking algorithms of *The West Wing* are presented not only as benign but as beneficial, other fictional depictions like *Minority Report* and its nearly-real crime-anticipating technology present technology in government as far more nefarious (Asher & Arthur, 2017). The vast potential of algorithmic regulation may seem steeped in science-fiction, however, it may be closer than we realize, which is why the relationship between technology and governance must be explored as technology – and access to technology – advances closer and closer to these fictional scenarios.

This thesis seeks to provide a theoretical investigation of the changing role of governance in response to modern levels of increased technology and algorithmic regulation. By examining cases in modern-day US within the past decade, we can take this debate out of the realm of science fiction and into the reality of the predictive analytics used to combat gun violence and child abuse in Chicago, Illinois. How the programs work and how they are being used is essential to understanding what the effect of the use of such technology in governance – especially when, like in Chicago, the programs are being utilized to attempt to predict the future behavior of constituents. To establish a better understanding of this relationship between government and technology and how they operate together in society, this analysis will be guided by the following question:

> How does algorithmic regulation alter the relationship between the US government and its constituents?

With emphasis on the role of government, the question will be explored through establishing an understanding of how algorithms operate, the history between algorithms and society, followed by an analysis of the US government's use of algorithmic regulation in Chicago, Illinois to combat the societal threats of gun violence and child abuse. The selected case studies represent the broader use for algorithmic regulation across the US – and worldwide – as a unique, modern

response to modern problems, but one that contains dangers of its own. Chicago operates as a stand in for any city across the nation or world that utilizes the algorithmic regulation and the theoretical discussion will touch upon the governmental theory behind the use of algorithmic regulation that can be applied anywhere.

Entrusting governance to algorithms has both potentially numerous benefits and potentially dire consequences. While an increase in technology represents an opportunity for greater security and efficiency, it also provides potential opportunity for increased biases and systemic prejudices. Algorithms are fallible technology and combining them with regulation and governance – even democratic governance – creates a greater societal risk. What happens if they do not work as they should? As Robert Jackson put it in his discussion of the potential pitfalls of global governance: "When the Leviathan does not perform as expected, there is usually hell to pay." (Jackson R. , 2007).

1.2 Theoretical and Methodological Framework

1.2.1 Theoretical Framework

The theoretical basis of the problem formulation relies on governmental theory on the role of government in relation to its constituents. For this, the works of post-modernist philosopher Giorgio Agamben and post-structuralist philosopher Michel Foucault have been selected for their prominence within the field and for their engagement with changes in governance through time as well as the resulting changes in the power dynamics inherent in the shift. Agamben, best known for his engagement with *biopolitics* and his concept of *bare life*, contends with the role of government in relation to citizens as well as with the powers dynamics within governance explored by Foucault. Foucault, famous for these explorations of power and its dynamics, provides a critical presentation of the changing role of governance through time and how these changes result in newer ways for the government to exert power over those it governs. These philosophers provide the backing to the argument that government can – and does – change, affecting the way it interacts with constituents. The concept from the newer academic branch of Science and Technology Studies (STS) of 'anticipatory governance' provides a name for this

new phase of governance in modern society and addresses the issues created by such a trend in governance.

1.2.2 Methodological Framework and Case Study Selection

This thesis explores the theoretical role of democratic government in a society with higher levels of technology. Theory will be utilized to establish that the role of government can change and to reveal the anticipatory trend in modern governance. This thesis then assumes there are two basic arguments in the debate over algorithmic regulation: 1) those that believe that the increased security gained by the technology is worth the risk created and 2) those that believe the technology represents a threat that is too great compared to the potential violations and risks. The following case studies and analysis exercises the caution possessed by the latter group but maintains a search for the benefits recognized by the former, seeking to maintain every possibility: the one side may be correct, or the other, or potentially even both.

The primary form of methodology will be a comparative analysis of two case studies in the US city of Chicago, Illinois. The use of case studies was selected due to the adaptive and comparative advantages the methodology offered through their use (Blatter & Haverland, 2012). Case studies allow for a more specific look at what is guiding and motivating the actors at play – in this case, largely, the Chicago Police Department and the Department of Child and Family Services – that cannot be as effective in a larger study (Blatter & Haverland, 2012). The nature of small case studies also permits a greater allowance for a "broad and diverse set of explanatory factors" that can lead to a better understanding of reality (Blatter & Haverland, 2012, p. 420). In a topic strife with debate and largely presented through media outlets and stories, tracing motivational and explanatory factors is the only way to fully understand the issue.

The selected case studies are based upon the algorithm-based programs that generates the Strategic Subject List, designed to prevent gun violence in the city and the Rapid Safety Feedback program previously utilized in social work for predicting child abuse. These case studies were selected because of the extensive nature of the technology used and its predictive properties, as well as for its use to prevent a serious social issue that has not been fixed by the use of other methods. These programs represent the strongest sides of both arguments and allows for a deep exploration of the role of the role of the Illinois state government in the issue and

implementation of the technology. The first study program is still in use in Chicago today. The second case study is not but is based on technology continuously utilized around the country. The Rapid Safety Feedback program features many of the same aspects as the SSL, however, it has been met with greater governmental scrutiny and has been removed in Illinois. This case study allows for an autopsy of the use of the program in Chicago, its continued use elsewhere, and a critical study of the flaws viewed by both the public and the government.

The empirical data has been gathered through the analysis of newspaper articles, public surveys, and governmental reports from the Illinois state government and police reports from the Chicago Police Department. As the research is reliant upon public opinion, newspaper articles from both local and national papers provide a glimpse into public reaction as well as official statement made by police and governmental officials. The newspaper articles depict the timely responses that occurred to these programs and allow for analysis of events as they happened over the past few years, tracking any changes in public and police response. Analysis of police data and reports – obtained through a Freedom of Information Act lawsuit in the case of the Strategic Subject List – allow for a look at the success and failure of the programs themselves. This empirical data shows the results of the programs which can be compared to crime rates in the area to establish the effectivity of the algorithm, an important part of calculating their cost to society and evaluating their role. The use of this type of anticipatory governance can then be evaluated in relation to the theoretical governmental role in modern society, including the government-technology relationship and the government-citizen relationship.

1.3 Preview

In chapter two, Theory, the theoretical framework will be expanded upon and the work of Agamben and Foucault will be explored in relation to government and power. These ideas, cultivated by well-known theorists, will be paired with the newer genre of Science and Technology Studies and how it explores the relationship between government and technology through the utilization of the concepts of ‘anticipatory governance’ and ‘algorithmic accountability’.

In chapter three, Context: Algorithms and Society, background on algorithmic regulation will be provided, including its use and application throughout the past few decades both governmentally

and socially. Additionally, algorithms themselves will be defined and the technology that operates them explained. The case studies of the Strategic Subject List and the Rapid Safety Feedback programs, both utilized in Chicago, Illinois, will be contextualized in American governance and introduced to be analyzed.

In chapter four, Analysis, the case studies of the Strategic Subject List and the Rapid Safety Feedback programs will be analyzed through four identified themes of security, privacy, efficiency, and effectivity. These case studies and themes will be analyzed through Agamben and Foucault's philosophies, with empirical data found through newspaper articles, primarily from the *Chicago Tribune* and *The New York Times*, as well as public reports from the Illinois state government and the Chicago Police Department.

In chapter five, Discussion, additional aspects of the discussion on algorithmic regulation will be explored. This includes an assessment of the relationship between algorithmic regulation and the Turing test including a thought experiment on the potential of an algorithm with the same failure rate as a human. Additionally, the role of algorithmic regulation as a global concern – and not simply an American problem – will be established and explored through a brief comparison to European Union regulation.

2. Theory

To study the role of the government is also to study its power, including the way it exerts that power and to what end, as well as how it changes over time. For this reason, emphasis has been placed on theory that focuses on governmental power and change. When engaging with an issue like governance, with a past better measured in millennia than centuries, change is not a new dilemma. Within the history of global politics, changes in governance are simultaneously vast, dramatic, and occasionally, violent. The intentions, methods, and forms of governance around the globe have fluctuated with social and economic changes and revolutions. At one point within governmental history, democracy itself was a new idea. Since its inception, democratic governments have changed and adapted to an ever-changing world. The advent of new technologies like the printing press, artillery, the automobile, the computer, and more all have altered how a democratic government interacts with the citizenry that elected it. The explore this changing relationship, the theories of two prominent philosophers, Giorgio Agamben and Michel Foucault, have been selected for their discussions on the changing nature of the role of government in the modern era and the power struggles evident within those changes.

An Italian philosopher, Agamben is must well-known for his creation and exploration of *biopolitics* and *bare-life.* These concepts are critical in the study of the relationship between a government and its citizen by establishing the role of power in governance, especially in regard to the citizens or beings that exist within it. His 1995 book, *Homo Sacre: Sovereign Power and Bare Life*, famously engages with the topic and provided a complex new presentation of the relationships inherent within governance and the difference between being a person and being a citizen. Agamben's engagement with *biopolitics* and *bare life* and how identification of "political" beings assigns agency to citizens with political membership in democracies and takes a deeper look at what the citizenship in a nation means and entails, as well as how the citizens is treated by the government (Agamben, 1995). The ideas Agamben has presented are vast and therefore specific quotes have been selected for their relevance and concentrated application to the issues at hand.

French philosopher and social theorist, Foucault is well-known for his engagement with and study of power roles and dynamics. Despite protests of the labels in his life time, his work is often categorized in academia as a post-structuralist or post-modernist. Not only is his work

integral to discussions on power relations in government, Agamben utilized Foucault's work on the relationship between government and citizens in his own work. In his book, *Discipline and Punish*, Foucault engages with Jeremy Bentham's design of the Panopticon and the power relationships at play within it (Foucault, 1977, pp. 195-231). These relationships offer a tangible model of the potential of state and governmental power, especially in respond to changing levels of technology use within them.

With the creation of any new type of technology, the government must adjust to accommodate new rights or new prepare for new dangers. In the face of these changes, governments turn to regulation. As these regulations evolve and make up more and more of governance, it is important to explore the core role of government in order to evaluate how it has changed—or has not changed – in modern times.

2.1 Government-Citizen

In contextualizing the way a government's use of technology affects its relations to its citizens, the relationship between government and constituents must be explored. The following quote was written by Foucault and then further explicated upon by Agamben. It sets up the relationship between the government and those it governs. On this relationship, Foucault noted:

> "For millennia man remained what he was for Aristotle: a living animal with the additional capacity for political existence; modern man is an animal whose politics calls his existence as a living being into question" (La volonte, p. 188)" (Agamben, 1995, p. 3)

In establishing the long theoretical history behind the relationship between citizens and government – stretching back to the creation of modern-day government – Agamben presents Foucault's quote as a way of establishing how government has changed over time, becoming an entity with a power it was not initially set up to have. Agamben uses Foucault's point to engage with his own concepts of 'biopolitics' and 'bare life' (Agamben, 1995, p. 3-4) which both speak to a person's potential political agency within governance. However, Foucault's comment on the changing relationship also speaks to an important beyond point this; "it is also, by noting that the shift in the relationship between humans and government has moved so far that governments have the power to decide *who* is human, commenting on the increasingly intrusive role of the government in the lives of those it has power over." (Cook, 2017, p. 4). The remarks upon a

dramatic shift in the power of the government, swinging the pendulum in favor of the government and thereby reducing the power – including the political agency – of the governed.

Agamben goes on to emphasize this point, acknowledging the diminishing position of power of those under state control are in when he writes:

> "Everything happens as if, along with the disciplinary process by which State power make man as a living being into its own specific object, another process is set in motion that in large measure corresponds to the birth of modern democracy, in which man as a living being presents himself no longer as an object but as the subject of political power." (Agamben, 1995, p. 9)

This shift from 'object' to 'subject of' is a critical change in the role of governance – "especially in a democracy, where (at least theoretically) those being subjected to power are also capable of changing the system to which they are being subjected. Therefore, if something were to damage their trust in the system – in this case, the missing part of the triad: technology – they could change it. The critical sub-question then becomes: where is the line? What draws it?" (Cook, 2017, p. 4). In a democratic government, which party – government or constituent – truly holds the power? Both Agamben and Foucault's work points to the growing power of the state and the government as oppositional to the constituents. In this, any increase to the power of the state is a threat to the power of constituents and the introduction of new technology into state control certainly increases the power of the state.

2.2 Government-Technology

In response to the ever-increasing role of algorithmic regulations in real government and politics in the twentieth and twenty-first centuries, Agamben would later be quoted remarking upon the way governments utilize their technology – and for what purpose. Essentially, Agamben believes, governments can contend with causes and effects of the world around them. However, as governing the causes of societal issues and threats can be "difficult and expensive" (Morozov, 2014), the government often elects to engage with the effects instead. Because of this decision, governments must increase control over their constituents in order to temper the effects of societal issues while the causes behind them continue. Focus on effects lead to an increase of governmental control because, "Causes demand to be known, while effects can only be checked

and controlled" *(*Morozov, 2014). Algorithm regulation offers a check on these effects, but also represents the increase of governmental power necessary to do so.

As he engages with algorithmic regulation, Agamben is addressing the broader way technology and advances can be used by the government. Beyond considering the changing relationship in control between those under control and governmental agents, when considering advancements in technology, one must also consider how – and for what purpose – that government is working. If Agamben's above assessment is correct and governments are focusing solely on the effects of societal problems, not the causes, then the use of algorithmic regulation compounds the problem. Agamben's notion is expanded upon by the idea that "Algorithmic regulation is an enactment of this political programme in technological form" (Morozov, 2014), meaning that algorithmic regulation is effect-driven as well.

What are the consequences of an effect-focused, technology-based government? Certainly, "It may be possible to apply this thought to the algorithmic regulation debate in general: If a government is so focused on the outcome, or what happens through the regulation, will it – or, more specifically the politicians carrying out its actions – be critical enough about the *use* of the regulations?" (Cook, 2017; emphasis updated). Consider the bipartisan debate over Sorkin's fictional algorithm:

> On *The West Wing*, the debate starts with the census, the process is the very act of the government counting its citizens. In doing so it is deciding who is and who is not part of the that citizenry or population under its control, and, (however unintentionally) excluding certain parts of that population – for a myriad of reasons including race, socio-economic status, or even simply whether or not they answer their front door.
>
> Sorkin's debate, however, strikes a different chord mid-episode. After winning the census debate with opposing Congress members, one character is left to lament that the change toward algorithmic regulation is not perfect. In fact, he notes that it has potentially dangerous ramifications as well: *"I'm not wild about the precedent… What's to stop us from saying we don't need elections, we'll just use polling data. 1150 people with the sampling error of plus or minus three will decide who runs the country"* (Sorkin, 1999). (Cook, 2017, p. 5)

This concern is present outside of Sorkin's fiction universe – it is echoed in those who are cautious about the use of algorithmic regulation and its implications will be echoed in the upcoming case studies in Chicago.

The relationship between government and technology – including the way constituents vote (Sanahuja & Ghia 2015) – desperately needs further exploration as the two become more and more intertwined. The way government uses its power – especially the power gained through advances in technology such as mass data collection and algorithmic regulation – is not only a question of whether the government *should* use that power, but how *much* it should use and how that level affects its subjects and those under its control. Perhaps, collectively, we might decide that the use of algorithmic regulation is acceptable for a census. Its use for voting, however, may appear more suspect. This means there is a line between how much technology we, collectively as a society, accept from our government and how much we do not. How exactly does a society decide on that line? What about a world were algorithmic regulation encroaches upon every aspect of government? Pushed even further, how about a government with an almost omnipotent role in its citizenry's lives? (Cook, 2017)

Foucault and Bentham's Panopticon

When studying the government-technology relationship – particularly *how* government uses technology – Jeremy Bentham and the notorious Panopticon is a common point of departure. Both its historical usage and the academic theories and studies surrounding it, have created a mythos about the prison format in the media today. When Foucault wrote about the Panopticon in *Discipline and Punish*, he was writing about the power dynamics at play within it: one centralized source of total power, with ultimate control over the subjects surrounding it (McMullan, 2015). The shape of the Panopticon, a central tower with a complete visual access to the numerous cells that surround it on all sides, lends it easily to the parallel of governmental control (Foucault, 1977, p. 3). If the central tower in the government and the cells that surround it are citizens, the Panopticon represents an end of the spectrum, the full potential of the citizen-government relationship when vast technology is introduced. It may be Orwellian, but the Panopticon does represent the potentially nightmarish reality that vast algorithmic regulation and

technology advancements could create – perhaps with the potential to do so more quickly than we realize. This looming threat reminds us once again of the relevance of considering the power relationships with the Panopticon.

This was not the goal of the Panopticon, however, to model a scenario of total governmental control. Bentham's original concept, based in his strong belief in utilitarianism, was a model based on achieving the greatest amount of success with the least amount of effort (Campton & Elden 2007). In this case, 'success' was the complete surveillance of the prisoners. With the new format, numerous prisoners could be monitored by a single guard. The benefits of this format are clear: it is cheaper and more efficient. The psychological (or even physical) well-being of the prisoners was hardly a concern of the time, and it we remove it from the analysis, the Panopticon works as it was intended. From this perspective, it is all about efficiency and effectivity.

However, as Foucault focuses on in his work, in both practice and theory, the physiological aspects cannot be ignored. The power-dynamics at work inside the Panopticon represent some of the most studied dynamics for decades. How these relationships work and what makes them work is critical. A key aspect is *visibility* (Cook, 2017). The prisoners – or citizens – on the periphery do not know if they are being observed by the central tower or not – but it is crucial that they are keenly aware that they *could be*. To put that power relationship into a modern context:

> Continuing with Sorkin's census, if the algorithm were fully explained (or access to an explanation could be achieved) and the public knew the census was being carried out in this new way, it might represent an acceptable use of algorithmic regulation. However, in the far more literal case of CCTVs, what happens to the population when the government has the opportunity to see anything happening in a public space at any time (McMullan 2015)? There is no way to know if someone is monitoring a particular CCTV electronic feed at any given moment, but there is always the potential. Pushing even further, into data collection, what about when a subject does not know they are being watched at all (McMullan 2015, Sanahuja & Ghia 2015)? This has the potential to change the way the revised Panopticon would work – and perhaps test the way we use Foucault's theories about visibility and transparency – in a modern world. (Cook, 2017, p. 6)

The Panopticon's other key feature is the inescapability of the power at the center (Cook, 2017). The members of the periphery are under its total control – both actually and potentially. They remain *subjects* to the power – to combine Agamben and Foucault, they are subjects to Agamben's new form of government. This combination has been explored before, as well as updated to reflect modern considers. In an analysis of the ideals and realities of cosmopolitanism, Sanahuja & Ghia hypothesized possible responses from Bentham and Foucault about the updated concerns, like big data and data collection, their philosophies and theories address:

> From Bentham's perspective, it is an excellent result: a democratically elected government can improve people's actions without threats or bribery, merely by observing them more accurately … governments become more efficient and effective through their use of data. But from Foucault's perspective, the new data-driven behavioral economics is the epitome of a nightmare Panopticon. Precisely because the power is soft, imperceptible, cheap, and ubiquitous, it is not resisted. (Sanahuja & Ghia, 2015, p. 165)

Criticism of this assessment could come from its simplistic – or perhaps idealistic – understanding of democracy. Bentham's fictional assessment may have been accurate – in a pure democracy existing with any obstruction or corruption (Cook, 2017). This is never the reality, of course. If the power-dynamic created in the model was reliant upon that form of governance, the entire system would be suspect (Cook, 2017). The concern attributed to Foucault is far more realistic than Bentham's alleged idealism:

> This certainly speaks to the common negative connotation of the Panopticon and its relationship to governmental surveillance and data collection. Without assurance of a flawless democracy – which one assumes is not present – the powers behind the Panopticon become a dubious, if not monstrous, model and therefore the power dynamic they control becomes a potential threat as well. (Cook, 2017, p. 7)

However, there has also been criticism of Foucault's approach – and his use of the Panopticon – regarding technology and the modern world. Specifically, the criticism is the over-application of Foucault's panopticism in this field. "In the 2007 book *Space, Knowledge and Power: Foucault and Geography*, Jeremy Campton and Stuart Elden presented a book of essays questioning the inherent application of Foucault and the Panopticon to all new technologies. They also question whether scholars and theorists – particularly those that focus on surveillance – do not "assume

too much" in their analysis (Campton & Elden 2007, Wood 2007: 257)"[1] (Cook, 2017, p. 8). In a more specific study of the effects of a totalitarian governmental control of technology, this critique would be critical. However, in accessing the power relationship at play in the governmental-citizen relationship, the Panopticon still serves as a representation of increasing governmental control as well as a tangible representation of change governmental power dynamics. The model itself has become synonymous with this type of governmental expansion, especially through the use of new and controversial technological methods, which warrants criticism of its use but does not negate or disqualify it.

2.3 Science and Technology Studies (STS)

One of the complications of this issue is its relative newness within academia and governance itself. The relatively new field of Science and Technology Studies includes the study of technology within governance and its creation and use of modern governmental theory often includes the buzzwords and phrases such as 'anticipatory governance'. In a journal article entitled, "Beyond participation: opening up political theory in STS"[2], University of British Columbia professor, Alfred Moore, lays out one of the defining features of the government-technology relationship: whether or not the technical is political. In this way, the overarching debate must take a step back – beyond Agamben and Foucault – to establish, first, if technology should even be considered within the governmental sphere. This broad question drives the entire

[1] "In the essay, "Beyond the Panopticon? Foucault and Surveillance Studies," the author heavily critiques the use of Foucault in topic surrounding technology and government. Even while continuing to use Foucault as support, the author – providing the names of additional authors that feel the same – criticizes surveillance studies for the over use of Foucault and the Panopticon, even citing Foucault's own role in the simplification of the model (Wood 2007: 250). As a replacement, he offers several "post-Foucaultian" theories, including Latour's 'Actor-Network Theory', as more nuanced approaches to the Panopticon, modern-day technology, and government (Wood 2007: 256). This perspective offers an opportunity to study not only the theories themselves, but also how we use those theories – previously and today – to understand the relationship between government, subjects, and technology." (Cook, 2017, p. 8)

[2] This journal article is a review of Mark Brown's book, *Science in Democracy: Expertise, Institutions, and Representation.*

discussion. Certainly, Moore writes, the feeling within the STS community is that "the technical is political" (Moore, 2010, p. 1) and, in fact, may go even further:

> "A pithy summary of this aspiration is that the technical is political, the political should be democratic, and the democratic should be participatory." (Moore, 2010, p. 1)

This makes note of the many factors that drive both technology and society today. It is not enough to note the technical is political – that those politics be within a democracy is a critical point as well. The relationships within a democracy complicate the issue even further. If a society is adhering to the ideal put forth by liberal democracy, where and how does increasing technology fit in? As the technology itself is unlikely to go anywhere, the next step is how the government reacts to it. The most common response is what governments do in response to most things: regulation. At least, that is governments typically to in response increasing technology within the population, the citizenry. But what does the government do about the technology within itself?

The complication here is the regulation itself – how it is being done and how regulation done by algorithms can be regulated itself. In the piece, "The importance of regulation *of* and *by* algorithm", Martin Lodge and Andrea Mennicken explore the relationship between general regulation and algorithms – and the flaws inherent within algorithmic regulation, noting that the role of "…computerised algorithms in generating new types of unintended consequences" (Lodge & Mennicken, 2017, p. 2). These consequences include biases and prejudices that can become programed into the system initially or over time, as well as an over-reliance on the predictions themselves. Lodge and Mennicken compare the results of algorithmic-driven programs to weather forecasts. Even with science- and data-driven forecasting models, "one day's 'perfect prediction' might be completely 'off' the following day" (Lodge & Mennicken, 2017, p. 3). This comparison reveals a greater issue of how predictive analytics and algorithms are viewed by society and how much weight is automatically given to their results. Acknowledging the fallibility and incapacities of technology is a critical point in the way society addresses algorithmic regulation.

This comparison to meteorology also addresses one of the flaws of the use of algorithms – they seek to automate, digitize, and anticipate aspects of governance that might not be suitable for such treatment (Lodge & Mennicken, 2017). When meteorologists fail to predict rain, people get

wet. When the government and its algorithms fail, the consequences can be much larger. This highlights a key issue presented by technology: algorithmic accountability (Lodge & Mennicken, 2017, p. 7). Accountability must be established for algorithms to exist and perform in a governmental sphere. Like all things, they must be monitored, studied, and assessed to make sure they are doing their job – and doing it well. The crucial takeaway is simple: "…regulation via algorithm requires regulation of the algorithm" (Lodge & Mennicken, 2017, p. 3).

To accomplish this, Lodge and Mennicken propose parameters – or regulation -- on what algorithmic regulation can do. Overall, this means broad categorizations about what AR should and should not be involved in, including assessments like this: "algorithms should not be set to make straightforward ethical choices, but should be programmed so as to make 'content-dependent' choices" (Lodge & Mennicken, 2017, p. 3). However, as governance moves forward itself – towards things like anticipatory governance – technology plays a greater role in accomplishing governmental tasks and even categories like that become complicated. Anticipatory governance, heralded as critical to the future of STS (Guston, 2014)[3], is an important crux in this issue as it represents a potential shift in governmental roles.

Similar to Agamben's assessment of the government's role in fixing causes or treating effects, the status of anticipatory governance defines what a government should be doing, what its role in society truly is, what weight is granted to the foresight it can promise, and how much power should be given to the technology that can "predict". It is the anticipatory nature that complicates the role. It is simply not a feature of government that could have been possible before, so early governmental theory cannot account for it without analysis and its presence coupled with the new technology makes for the potential for an evolution in the governmental role.

Agamben and Foucault's assessment of the increasing power within governance and the diminishing power of the constituent can be seen through the contemporary trend toward anticipatory governance, as well as the shift of the constituent from an object of governance to a

[3] It is important to note that Guston is writing about 'anticipatory governance' in a broader sense, not limited to actual governments. Instead, it is defined: "the art of foreseeing the spread of an innovation's effect" (Guston 2014: 220). His assessment includes institutions and companies, as well as governments, and how all interact with new technologies.

subject of governance. The focus on the effects of societal issues breeds the use of more effect-driven programs, resulting in a technical world that is highly political. Without further investigation – and possibly regulation – these technical politics run the risk of creating risky power dynamics, drastically altering the relationship between government and constituent. Even without taking it to the full extreme of the Panopticon model, the unstable relationship between the sides creates tension and the opportunity for algorithm regulation and other technologies to further tip the scales.

To explore this issue, it is occasionally necessary to look at a few of the sides of the government-citizen-technology triad separately. To explore the relationship between government and citizens, the critical voice in governmental theory of Giorgio Agamben and his works, 'The state of emergency' and *Homo Sacer: Sovereign Power and Bare Life* (1995) provide a discussion on the changes constituents face as governments gain more control. Agamben's engagement with the work of another crucial theorist, Foucault, combines their theories on the topic of the role of government – especially regarding the changing nature of the relationship between governments and citizenry and the power relationships created and explored within. The relationship between government and technology – and how an increase in technology results in an increase in power – can also be studied both through Foucault's analysis of Jeremy Bentham's Panopticon (Foucault, 1977, pp. 195-231). These philosophies can coalesce together for the theory behind algorithmic regulation and its combination with anticipatory governance, which represents a modern trend in governance that is often coupled with algorithmic regulation.

3. Context: Algorithms and Society

This chapter seeks to provide the necessary academic, technical, and historical context required for the analysis. As a modern invention, algorithms and algorithmic regulation has a growing place in academia and literature, especially as the technology's role becomes more and more prominent in society. Just as Agamben and Foucault present a government which changes throughout time, society's use of technology has advanced over time as well and, to fully understand their changing role, more coverage must be given to both how algorithms work and how they have been used in the past half a century.

3.1 Literature Review

As a historically new phenomenon, algorithmic regulation is also relatively new in academic and only recently come into prominence in literature. The majority of sources on the topic have been published in the past decade, with many sources published in the past few years as the role of algorithms has become both more prevalent and more public. It is that same public exposure that has brought the topic into non-fiction literature, where the overall mechanics of algorithms are presented, the societal implications discussed, and the debate has been brought to a broader audience. The mysteries and complexities surrounding what algorithms are and how they operate have made them a topic that extends beyond academia and found a place in mainstream discussions, debates, and texts. Websites and publications ranging from *The Huffington Post* to *Vogue* have published articles about algorithms, piquing interest in a population that might not have otherwise realized the technology's prevalence in their daily lives. In many ways, these two categories – academic and non-fiction literature – also mirror the conversation about algorithmic regulation at large, with one side focused on the outcome of the introduction of such technology and one side focused on the mechanics of how that technology operates.

The literature surrounding algorithmic regulation has increased exponentially in the past few years, especially as the public debate about it has grown. Even within non-fiction, the texts range from the informative (Pedro Domingos' 2017 *The Master Algorithm*) to the critical (Cathy O'Neil's 2016 *Weapons of Math Destruction*) and represent both the public's curiosity about this new technology and the seemingly inherent acquiescence – coupled with the also dichotomous and seemingly inherent distrust – that permeates society as well. Cathy O'Neil's recent book,

Weapons of Math Destruction, bridges the gap between outcome and mechanics by taking a look at the numerous ways algorithms decide aspects of our lives. Each chapter of her book investigates a different category, ranging from banking to insurance to college acceptance, and identifies the risks and biases created by the algorithms at work in them. As a Harvard doctoral graduate and Columbia University professor, O'Neil draws on her experiences in pre-2008 Wall Street to interrogate the algorithms that not only run the banking industry, but also our society as a whole. Her work is highly critical of the entire apparatus and the automatization of society, though she notes it cannot be undone and the best solution moving forward is to regulate out we as society use algorithms on a day to day basis – a theme common amongst texts about algorithmic regulation.

Similarly, in 2017, The Centre for Analysis of Risk and Regulation at the London School of Economics and Political Science published an anthology of eights texts that explore algorithms entitled "Algorithmic Regulation" and featuring essays such as "The importance of regulation *of* and *by* algorithm" by Martin Lodge and Andrea Mennicken, "The practical challenges of regulating the quality of public services with algorithms" by Alex Griffiths, and "Evaluating predictive algorithms" by David Demortain and Bilel Benbouzid. These texts delve deeper into the more recent governmental aspects of algorithmic regulation (Lodge & Mennicken, Griffiths; 2017) than O'Neil, but also address several of the same algorithm-driven programs in use by police forces such as PredPol and HunchLab (Demortain & Bendouzid, 2017). Overall, the anthology is also highly critical of how algorithms are used today and the lack of regulation surrounding the use of algorithmic regulation around the world. Like O'Neil, it acknowledges the ubiquity of algorithms in today's society, continuing an argument that it is not that algorithms *are* used, but *how*.

Karen Yeung's – whose piece "Making sense of the European data protection law tradition" was also published in the LSE anthology – 2017 article "Algorithmic regulation: A critical interrogation" is another example of the very recent work being done in this area. As the title suggests, Yeung's piece provides not only a primer on algorithmic regulation itself but also a far more in-depth study of algorithmic regulation, how it works, and the role it plays in society and governance. She focuses on "pre-emptive" (Yeung, 2017, p. 14) algorithmic systems, a concern that is echoed more broadly by David H. Guston's 2014 article "Understanding 'anticipatory

governance'", which engages with the theme touched upon by O'Neil, the anthology, and Yeung: the expanding role of governmental responsibility for increasing technology.

Throughout the literature, two threads become clear: 1) inherently, as a society, we should not entirely trust the use of algorithms, and 2) the use of algorithms in governance through algorithm regulation and its implications should be further studied. A notion of distrust of the use algorithm regulation – and its ubiquity in our society – is clear, however the vastness and depth of the issue means that this technology requires checks against its power. Seemingly, algorithmic regulation has crept into society without a lot of attention or fanfare, but as Lodge and Mennicken point out, that does not mean it can be allowed to operate without restriction. The systems are already built around this this system and it is unlikely – if not impossible – to complete extricate the current system from algorithmic regulation. Instead, the response to these critiques seem to call for an assessment of the government's use of algorithmic regulation and its responsibility to this new and growing form of technology.

The overwhelming theme in the literature about algorithmic regulation in modern governance is that this form of regulation requires regulation itself – regulation that is lacking globally currently. To establish the kind of regulation, however, it is necessary to understand how the governments utilizing such technology interact with their constituents and requires a better understanding of the theoretical role of government. In the available literature, most focus is placed on mechanics and outcomes, not theory and governance. As this topic is an important global issue that either does affect or will affect nearly every government and all their constituents, this is a topic that deserves more attention. This thesis seeks to contribute to filling this gap in the literature.

3.2 What is an algorithm and how are they used?

In its colloquial usage, the word 'algorithm' represents a seemingly nebulous concept of mathematical functions and operations.[4] In his book *The Master Algorithm,* Pedro Domingos

[4] The pure definition of 'algorithm' is closer to "a set of guidelines that describe how to perform a task" (Brogan, 2016), which means that, in actuality, "even something as innocuous as a recipe or a list of directions to a friend's house can be understood as an algorithm" (Brogran, 2016). In its modern use, however, the word has become synonymous with a computer algorithm.

gives this simple definition: “An algorithm is a sequence of instructions telling a computer what to do” (Brogan, 2016). Therefore, algorithms exist ubiquitously throughout modern life. They decide what you see on social media, when you hit a red light, even your insurance rates. On any given day, you interact with hundreds – or even thousands -- of algorithms, deciding aspects of your life without you even being aware of them.

In this way, humans have been affected by algorithms since the invention of the computer. Governments have been interacting with algorithms through code-breaking since the cracking of Enigma. Historically, in this way, military and law enforcement have some of the earliest instances of algorithmic regulation – generally used in attempt to annihilate a threat or increase domestic security. As access to computer expanded, so did the public’s interaction with algorithms.

Through computer technology, algorithms already exist across numerous aspects of governance – because so many aspects of technology rely on algorithms, which make up and drive systems like databases, search engines, and smart phones**.** The accumulation of data through these methods (algorithms) and its use for governance (regulation) represents a changing mode of technology. While the mathematics behind them are nothing new, its use for governance through algorithmic regulation is, historically, more recent – stretching back a few decades. The implementation of technologically – and, more specifically, algorithmically – based law enforcement in the US dates back to at least the 1960s, when the New York Police Department’s (NYPD) ‘Operation Corral’ – Computer Oriented Retrieval of Auto Larcenists[5] – was first used to target criminals for car-related offenses (Morozov, 2014). The technology debuted in 1965 and utilized a license plate database and search engine to identify offending vehicles.

Operation Corral’s process was simple, but it did require a long bridge in order to be effective. Acting as a way to restrict the travel path of the suspect, the bridge would allow for a police

[5] It is noteworthy that, despite the acronym correcting spelling out ‘coral’, the operation was labelled ‘corral’, which has a definition meaning to gathering together in one space. While it is also a word commonly applied in ranching and animal rearing, in reference often to cattle or sheep, it also refers to the operation’s method of ‘corralling’ suspects on a bridge. The implications of the name, however, remain. While the nomenclature of these programs is not the focus here, it is interesting how the NYPD choose to name the program behind its first use of database-driven police work.

officer placed at one end to call the numbers of license plates in to a typist who would use them to search the database of the license plate numbers of over 100,000 wanted vehicles. If any of the license plates were found on the list – a process that was reported to take under seven seconds – the typist would alert a second police officer stationed at the other side of the bridge. That office could then pull the car over and potentially make an arrest of the suspect (Morozov, 2014). This now-seemingly cumbersome process – including three different players and two phones – represented a huge advancement for technology in law enforcement at the time.

By the 1970s, algorithms began to be utilized in college admissions offices came and this practice into prominence. The same technology had been used by governmental agencies like the Pentagon for years and as technology accessed increased, it was used to established who gained entranced into schools. While its use simplified the process for universities, it also brought up nuances the algorithms might miss or prejudices they might perpetuate. Take this example from former Data Practices Director at Columbia, Cathy O'Neil, in her 2016 book *Weapons of Math Destruction*. When St. George's Hospital Medical School switched to a digital admission process in the 70s, the institution encountered numerous problems with the ground-breaking technology, heralded for its sophistication but that also included a spell-checking feature that eliminated applicants with foreign names:

> St. George's already had voluminous records of screenings from the previous years. The job was to teach the computerized system how to replicate the same procedures that human beings had been following. As I'm sure you can guess, these inputs were the problem. The computer learned from the humans how to discriminate, and it carried out this work with breathtaking efficiency. (O'Neil, 2016, p. 248)

But this did not quell the movement toward further use of algorithms. In the 1980s, Wall Street and the American housing market entered into a Faustian bargain leading to disastrous effects decades later. The creation and marketing of mortgage-backed securities became a huge money-making industry – reliant upon the risk-analysis algorithms that falsely promised their status as secure (O'Neil, 2016) When the charade came down years later, the algorithms did not offer much aide. As O'Neil put it: "The math could multiply…but it could not decipher" (O'Neil,

2016, p. 107). In this case, not only did the reliance on risk-analysis algorithms fail to do its task, it failed to see an even bigger risk looming in the future.

In the 1990s, algorithms became a staple in police work across the nation. Predictive analytics, particularly based on locations, became a staple in the NYPD and other police forces around the country. This represented a shift in how much of police work was done. The introduction of these changes was followed by a drop in violent crimes in several major US cities[6] as well as public outcry and accusations of bias and profiling (O'Neil, 2016). Many of these programs are still in use today and their mechanics will be engaged with later. In fact, not only are many of these programs still in use still the 1990s, the use of these programs has only grown in the past three decades. Despite entering a new millennium, the 2000s maintained many of the same techniques and strategies, relying even more on predictive analysis than any other time in history. After situating their use in within a more specific American governmental context, the use of these programs will be explored more in-depth in the following case studies based out of Chicago, Illinois.

3.3 American Context

The current American government was created in 1779, three years after declaring independence from British rule. This Constitution laid out a new federal government: a democracy with power over thirteen states in New England. While the federal government maintained certain powers -- such as foreign diplomacy and declaration of war – the states were also given powers to act as a check on the federal government. These powers were extended in the addition of the Bill of Rights in 1791[7] and included the line:

> The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.

[6] This does not verify that the decrease in violence crime was directly correlated to use of these programs, however. The relationship is time-based, but not necessarily causal.

[7] The Tenth Amendment states: “The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.” (US National Archives, 2018)

Since the addition of the Bill of Rights, sixteen other amendments have been added to the US Constitution, including: the 13th which abolished slavery, the 18th which created prohibition (and the 21st which nullified it), the 19th which gave women the right to vote. Amendments 16 and on were added in the twentieth century, which the most recent amendment added in 1992.

Historically, Cambridge University professor David Runciman appears to be correct in his assessment that the American "political system has hardly changed at all since 1989" (Runciman, 2014, p. 63). First established in 1776, the government itself is only 242 years old. Compared to Athenian democracy, it barely registers on an historic scale. But when considering advancements in technology, a decade can bring about huge changes and two centuries is bound to require some updates. For context, in the 1770s, the latest technological innovations were the Franklin stove[8] and indoor toilets (Palmer, 2014). The printing press dominated in the media and wearable tech was limited to a pocket watch – that needed to be winded. It was in this technology environment that the new US government – then presiding over approximately two million people[9] – as written into existence by the Constitution, establishing a system to protect "life, liberty, and the pursuit of happiness" (US National Archives, 2018). Since its inception, however, the system has meet with two centuries of technological change – including the creation and implementation of algorithmic regulation. In a time even before automobiles, the governmental system set up in the Constitution was designed to be run by, well, humans. In fact, even Runciman's more recent assessment of governance in 1989, places the current system created without awareness or even anticipation of the iPhone. As the technology became available, however, the government became to incorporate it. The following case studies present algorithm-driven programs that have been utilized by the state government in Illinois and the Chicago Police Department within the past ten years.

3.3.1 Case Study One: Strategic Subject List

Chicago, Illinois is the third largest city in the United States and is home to nearly three million people in the metropolitan area. Historically known for bootleggers, gangsters, and jazz, modern-

[8] The Franklin stove changed colonial life as well as the way food was cooked by utilizing the new invention of rolled sheet metal to create a fireplace that was designed to provide heat in the winter but also allowed for the elimination of smoke while cooking (Palmer, 2014).

[9] This number is taken from the website for the United States' Census Bureau, which reports 2.5 million residents living in the US at the time of independence.

day Chicago is also known throughout the country – and the world – as a hotbed of violence and homicide. Actual crime rates in the city have fluctuated in recent years, rising to a historical spike in 2016 – the bloodiest year in Chicago since 1996 – and have sparked criticism of local police (Sweeney, Schmadeke, & Meisner, 2017). 2017 reported 650 of homicides, down from over 750 in 2016, but still revealing a serious problem with violent crime (O'Connell, 2017)**.** In fact, in recent years, Chicago has represented a deviation from other major US cities such as New York and Los Angeles that have seemingly quelled the rise of violence. This is not to say these cities do not have violence[10], but their gun-related homicide rates have plateaued or even fallen recently. In Chicago, however, according to the statistics in recent years, gun violence is on the rise. In comparison to New York, another diverse city with a similar homicide rate in the early 90s, by 2016, Chicago had three times the number of homicides (Sweeney, Schmadeke, & Meisner, 2017). What could account for this? According to a New York Times report, the answer is clear: guns. When guns are not involved, New York's homicide rate is actually higher than Chicago's, "but when it comes to shootings, both fatal and not, Chicago stands out" (Fessenden & Park, 2016). In response to increasing criticism from both the public and the federal government, the Chicago Police Department (CPD) has spent part of the last decade introducing new technology-based initiatives into police work in increase the force's effectiveness against gun violence.

Known in the US as something of a liberal bastion – former US President and leader of the Democratic party, Barack Obama represented Illinois in the US Senate from 2005-2008 – and often cited for its gun control laws, Chicago's fight against gun crime has garnered both national attention and criticism. After threatening to do so earlier in the year, current US President Donald Trump sent federal assistance to Chicago in June of 2017 in an effort to address the gun violence (Nelson, 2017). Nationally (and internationally) harangued politically and in the press, the situation in Chicago did need new tactics. In a press conference, Chicago mayor Rahm Emanuel addressed the issue and mentioned the new technology the CPD had been – and would

[10] All three cities reported over 30 homicides per 100,000 people in the early 90s. However, since 1995, the rates in both Los Angeles and New York have almost consistently dropped to 7 and 4, respectively – a small peak in the early 2000s in Los Angeles not withstanding – and are both half the rate of Chicago's 17 out of 100,000. (Fessenden & Park, 2016)

be – employing to fight the increasing crime rate. He was careful to mention that "the expanded technology is only one of the piece in the city's fight against the shootings and violence that have landed Chicago in the national spotlight" but emphasized how new tech-based programs could greatly increase the effectivity of the CPD (O'Connell, 2017). These new initiatives, including ShotSpotter a program that "captures audio of gunfire and attempts to pinpoint its location" (O'Connell, 2017), include the use of algorithm-based programs designed for law enforcement:

> [Chicago police Superintendent Eddie Johnson] said the upgraded technology is part of the department's "data-driven enforcement," which compliments police community engagement efforts. ShotSpotter technology alerts officers to possible gunfire before 911 calls are made and allows detectives to pinpoint crime scenes for collection of bullets or shell casings…The Police Department has used the ShotSpotter occasionally in the past decade. Former Superintendent Garry McCarthy touted the system in 2012. Prior to that, the city twice installed the devices but ultimately removed them because of their high price tags and ineffectiveness. (O'Connell, 2017)

However, the recent crime waves in 2015 and 2016 have the department returning to embrace these types of programs, despite their flaws. While many of the programs utilized around the US are location-based, like ShotSpotter, seeking to find and stop crime occurring in specific areas, the CPD has also introduced an entirely new program with a different approach and a broader scope: the Strategic Subject List (SSL).

The SSL, colloquially referred to as "the heat list", was first created in 2013 by the Illinois Institute for Technology and refers to a compiled database of citizens ranked by their propensity for – or proximity to – crime. Instead of tracking crime in a specific *location*, it focuses on the identification of the *people* likely to be involved in gun violence. Essentially, the algorithm behind the SSL seeks to "predict who is most likely to be involved in a shooting, either as perpetrator or victim" (Asher & Arthur, 2017), a task it accomplishes through the use of risk factors analyzed by a computer. At its base, the program is simple: the list is generated through the use of a computer algorithm designed to take into account past behavior – largely arrests and convictions – and assign a risk score ranging from 0-500. The information for hundreds of thousands of arrested individuals has been run through the algorithm, ranking them by risk

factors for gun violence. In 2016, nearly 400,000 people were on the list (Chicago Police Department, 2016).

With the data collected, the CPD has reported that it has been able to identify 1400 of the highest-risk candidates – although the algorithm apparently does not differentiate between those most likely to use a gun themselves or be victimized by one (O'Connell, 2017) – in the Chicago-area. This identified list is critical, the CPD say, because the violence in the city is concentrated to a small percentage of criminals. In fact, this reasoning is part of why the SSL was created in first place, after Yale sociologist – and Chicago native – Andrew Papachristos claimed the city's high crime rate was likely due to a small group of offenders in high-crime neighborhoods (Gorner, 2016). Some recent statistics appear to support this hypothesis: in 2017, "more than 70 percent of the people shot in Chicago were on the list, as were more than 80 percent of those arrested in connection with shooting" (Davey, 2016). Police believe that in the city of 2.7 million, 1400 offenders are responsible for the majority of violence and the SSL allows them to focus their efforts where they are needed the most.

Through the application of the SSL, the CPD has also been able to pinpoint over a thousand of these 'candidates' to receive visits at home from the police. While the list largely focuses on the top four hundred identified citizens**,** around 1300 of those identified by the algorithm received police visits in the last three years – and the CPD plans on increasing that number by over one thousand visits this year (O'Connell, 2017). These visits serve to inform citizens not only of their status on the list, but to "bluntly warn that the person is on the department's radar" (O'Connell, 2017). These visits are viewed by the CPD as a deterrent to potential future crimes perpetrated by those on the list, however they have also been met with skepticism by those who criticism the SSL and its fallout.

The SSL is still in use in Chicago today.

3.3.2 Case Study Two: Rapid Safety Feedback

Gun violence is not the only issue the American government has responded to with algorithms and predictive analysis. After the deaths of nine children in the foster care system prior to 2013, Hillsborough County, Florida, which includes Tampa, introduced a new program entitled Rapid Safety Feedback (RSF) designed to identify households at risk for child abuse (Levenson, 2015). This type of program has gained national attention in recent years and is used throughout the US.

The way the RSF works is very similar to the SSL, including the data mining of child services records and the generation of a "risk score" for the probability of the child's severe injury or death due to child abuse within the following two years. The Hillsborough model was developed based on the analysis of 1500 cases, including the cases of the children who died, and the establishment of the factors in the home that presented the greatest danger to the child's welfare. This model found that the worst cases often had similar patterns and features such as young children, a boyfriend living in the home, a history of drug use or domestic violence, or a parent that had been in foster care (Levenson, 2015). These identifiers are then applied to rest of the cases to search for children in homes that may be at-risk for children abuse and violence.

Like the SSL, this program also includes the generation of a "risk score" for the probability of the child's severe injury or death due to child abuse within the next two years – and it has received a similar backlash for its implications. The generation of the score in both cases to designed to reveal where government officials should place most of their resources or attention. In the case of social workers, who increasingly oversee more and more cases at once, the program provides a way to highlight the homes – and children – who have the greatest likelihood of abuse. Rapid Safety Feedback evaluates all the families on the same factors, supposedly eliminating social worker's individual biases and creating a faster, more efficient way of identifying potentially dangerous environments.

Social work is often identified as a career with high stress and high workloads. The Illinois Department of Child and Family Services cites large workloads as a continuing issue with its staff as well as one of the reasons it turned to predictive analytics (Jackson & Marx, 2017). Like Hillsborough County, the department introduced the program after multiple child-abuse related deaths in 2015 (Jackson & Marx, 2017). With intentions to streamline the social work involved, the RSF seemed to offer a way to identify the most at-risk children and insure that departmental resources were being applied in the most effective way.

This is the pitch for the use of these programs: that an algorithm can do part of the work a social worker could and therefore can increase productivity. Head of the child-abuse center at Children's Hospital in Pittsburgh, former research-lead at the federal Commission to Eliminate Child Abuse and Neglect Fatalities, and proponent of algorithm-based programs like the RSF, Rachel Berger, equates the process of identifying the factors involved in abuse not to just finding

a needle in a haystack, but to finding a specific needle in a pile made entirely of more needles (Hurley, 2018). Because of the difficulty and complexity of this work, Berger believes the algorithm provides a more concrete and precise result than human-based social work. “It’s finally bringing some objectivity and science to decisions that can be so unbelievably life-changing,” Berger said about the use of predictive analytics in social work and child abuse investigations (Hurley, 2018). On a grander scale, advocates of the technology agree and say, “if it is possible to use big data to spotlight a child in trouble and intervene before he or she is hurt, then doing so is the government’s moral obligation” (Jackson & Marx, 2017).

Around the nation, many states are using the RSF, and other programs like it, in social work and family services. Recently, in 2017, Chicago ended their use of the program, citing ineffective results (Jackson & Marx, 2017). After implementation and the data mining of their files, the Chicago Department of Children and Family Services (DCFS) child welfare officers were given reports totaling in the identification of over 4,100 at-risk children in the Chicago-area were probabilities of death or injury in the next two years at over ninety percent (Jackson & Marx, 2017). Within that number, 369 children under the age of nine were given a hundred percent chance of death or injury (Jackson & Marx, 2017). This statistical generation was met with suspension and panic by the DCFS and, after two years of use, the Chicago department office announced in December of 2017 that the use of the program would be terminated.

4. Analysis

These two case studies will provide examples of what US governmental departments have accepted and rejected from predictive analysis programs. Through analysis of local and national new reports, articles, and public releases about the use of the SSL and the RSF, four themes emerged as the most relevant in the discussion of use of the algorithmic regulation, predictive analysis, and the use of these programs by police and governmental services in Chicago. These emerging themes are: security, privacy, efficiency, and effectivity. These themes represent the core issues in establishing the governmental role in algorithmic regulation and the public – and political – debate surrounding it. The following analysis will utilize them to apply the governmental theories and philosophies of Agamben and Foucault into the debate surrounding algorithmic regulation in Chicago – and, more broadly, the use of these new programs in governance around the world as a reflection of the changing nature of governance and the relationship between governments and constituents.

The debate around the SSL, RSF, and governance – in this case, the more specific aspect of governance of policing – has two levels: 1.) what amount of technology the police should have and 2.) what the police should be aiming to do with that technology. In this case, the first level is simple: should the police create and have access to the SSL or should they not? Certainly, as a society, we have agreed that governmental databases are okay: things like the license plate data collection at the Department of Motor Vehicles, no-fly lists, and the sex offender registry all operate around database lists. If the SSL collects the information of arrested persons and compiles them together to create a list of those most likely to be party to crime, it is not too far of a stretch from other databases it creates despite its billing through headlines like, “With violence up, Chicago police focus on a list of likeliest to kill, be killed” (Gorner, 2016) and “Chicago’s Murder Problem” (Fessenden & Park, 2016). However, there is something about the SSL that grabs public attention unlike other registries. Perhaps it is its proximity to science-fiction and dystopian futures that have made the public weary of such technology. For whatever reason, this response has made the answer to the first level intertwined with that of the second. Essentially, how much technology the police should have is dependent upon what they are aiming to do with it.

On a larger scale, this issue is not limited to police work or Chicago. The use of predictive analysis has implications for governance on both the state and federal level throughout the US. While these case studies represent two examples of the way governments use predictive analysis and algorithmic regulation in response to gun violence and child abuse, the conversations about them can be applied on a broader scale. The themes of security, privacy, efficiency, and effectivity can be applied at both a state and federal level. While this analysis engages with case studies largely set in Illinois, it will contend with the wider implications of such technology changes as well. These case studies and analysis can not only provide a greater understanding of the programs, but the changing role of government as well to one that seeks to anticipate crime and predict not just where it will occur, but by which of their constituents may commit crime in the future.

4.1 Security

The first theme to be address is the one most prominently featured in the discussions surrounding the use of these two programs in governance: security. Both gun violence and child abuse represent serious threats that pose dangers to constituents of Chicago on a daily basis. They are also societal issues that seemingly cannot be solved with governmental – and, more specifically, legal – involvement. Therefore, these programs offer a new, potentially better, way to combat these issues and achieve a more secure environment. However, the debate grows as the most evasive nature of the programs is revealed and weighed against the protections offered by the technology. Are these programs truly protecting constituents? And, if they are, are they protecting all constituents equally?

To fully analyze this, one must first accept the premise that a government seeks to protect its citizens. The US Constitution preamble established a government seeking "….to establish, insure domestic tranquility, provide for the common defence, promote general Welfare…"[11] (US National Archives, 2018), which can be interpreted in many ways but certainly carves out a governmental role based in creating and maintaining a secure environment for the constituents living within the nation. It is exactly *how* that goal is achieved where the use of algorithmic

[11] Original spellings from the document have been maintained.

regulation is questioned. How far can, or should, the government go to create a secure environment? If the creation of this environment involves the violation of rights, is it really security at all?

How the government should go about insuring security is a topic addressed by Agamben who engaged with the question: Should the government focus on effects or causes? In these cases, this is to question: what purpose does the collection of data and creation of lists such as the SSL or the RSF serve? Does it alone solve the issue? Or does it merely engage with the symptoms and effects of such issues? It is possible, however, to bend this understanding in a way that Agamben likely did not intend: to truly address the issue, would we, as a society, have to accept a further-reaching governance? To engage with these questions, let us first consider what the SSL strives for security by addressing causes or effects, with Agamben's assertation that governments should seek to find solutions to causes in order to truly best serve their constituents.

As evidenced by the numerous press conferences and news articles published around the growing recent violence in Chicago, certainly the attention put on the SSL is a reaction to the increase in gun violence. Its very implementation is a reaction to the growing homicide rate in recent years. But it would be overly simplistic to stop the analysis there. Governments can – and should – react to crime. Chicago's introduction of the program reacts to an influx crime and does seek to solve gun-related homicide. Let us assume that this response does meant with Agamben's assertation: the problem is gun violence and the cause of that problem is criminals using guns. In that case, the SSL does achieve its goal in going after the cause. The data created by the SSL goes after criminals who cause gun-related violence. If those perpetrating crime are on the list generated by its use – and stats say that, to a certain extent, they are[12] (Asher & Arthur, 2017) – then the SSL is correctly identifying a direct cause of crime and seeking to solve it.

However, is that what Agamben meant? Is finding the criminals truly finding the cause? Or does addressing the cause of crime mean addressing what is driving those criminals to their acts?

[12] It was predicted that within the top four hundred names, one third would be involved in a gun-related crime in the following eighteen months. This prediction was proven correct by CPD statistics (Asher & Arthur, 2017). While this does not guarantee that the program always makes the correct identification, it does show that it is operating as expected.

What if we assume that other societal issues are the cause of gun-related violence. This would mean that Chicago is not treating the cause of the problem, but merely an effect. This outlook is backed up by studies comparing Chicago to other large US cities. A New York Times report on the violence in Chicago compared with New York made mention of a difference that may also affect the differing crime rates between the two cities: intensely racially segregated neighborhoods, an issue which is much worse in the Chicago area than in New York (Fessenden, 2016). Another article in the *Chicago Tribune* mentions poverty, unemployment, and a sense of "hopelessness" as factors in what causes people to turn to crime and violence (Sweeney, 2017). These factors alter the conversation about gun violence everywhere and shift the true cause of the problem. This means that, in order to create a more truly secure environment, the government would need to engage with these issues as well, in a more comprehensive attempt to end gun violence.

Top officials in the Chicago-area government, however, do not prioritize these issues over punishment for the crime themselves:

> [Chicago police Superintendent] Johnson said he was sensitive to the inequalities of the criminal justice system but feels consequences aren't dire enough to deter crime.…Johnson has an ally in newly elected Cook County State's Attorney Kim Foxx, who …wants to identify the most violent criminals and is looking to forge partnerships with academics to try to better understand the root of the gun problem.
>
> "We want to go after those who pull the trigger. We want to make sure that they are held accountable, and we also want to make sure that the next person who is thinking about picking up a gun doesn't," Foxx said. (Sweeney, 2017)

If the CPD adheres to Foxx's beliefs and seeks to prevent crime by using the SSL and deterring those most likely to commit crimes, then the SSL not only works and achieves their goals but is a necessary piece of the strategy. This deterrence-focused method requires more foresight and prediction which can only be achieved through new technology. This type of anticipatory governance coupled with algorithmic regulation does represent a new frontier in the role of democratic government and its policing. The usage of the SSL has the potential for that predictive analysis but in doing so creates a power dynamic similar to those proposed by

Bentham and discussed more theoretically by Foucault: a central power overseeing those on the periphery that do not know whether or not they are being watched any given moment.

The theme of security also includes addressing the issue of creating security for all. Just like humans, algorithms are capable of suffering from biases and prejudices – including those programed into them and those created by their results. In the 1990s, the NYPD introduced a new program called CompStat, short for 'Compare Statistics'. The program sought to more accurately pinpoint crime through statistical analysis. This data-driven police work has once again drastically altered how law enforcement works. The use of statistical could more accurately show where crime was occurring and create a seemingly more effective way to patrol. CompStat has paved the way for more modern programs such as PredPol and HunchLab, which allow police departments to more accurately predict where crime occurs down to areas the size of city blocks (O'Neil, 2016, p. 64). Such programs can go even further and use risk analysis software that notes the placement of high risk locations, such as ATMs and unattended parking lots, and calculates where the most crime *should* occur, statistically.

However, these policing methods and software programs like Compstat, PredPol, and HunchLab have been facing criticism, particularly the "pernicious feedback loop" (O'Neil, 2016, p. 65) they create: the algorithm says most crime should occur in location X, therefore it is patrolled more, resulting in more arrests which are then entered into the database and strengthen the statistical evidence that more crime does indeed occur at location X. In this, the software reinforces its own conclusions. This loop represents a very real danger associated with algorithms: statistical bias**.** Algorithms – or statistics that accompany them -- are not infallible. They are not pure math, existing on their own and creating some kind of truth. They are programed by humans, and, like those working in admissions offices, can therefore possess any flawed reasoning programed into them. They are also surprisingly simple functions that can serve to perpetuate their own analysis. As will be explored more in-depth later, they are not, however, static. They are capable of adapting, which is credited as a technologic breakthrough, but is also at risk for causing them to develop biases and prejudices both from the data put into them and the data they produce. An algorithms ability to provide security to all, therefore, is linked to its ability to adapt without these biases or its presence in an environment where its work will be double-checked and evaluated with logical reasoning beyond the binary of a computer.

Whether or not the SSL and the RSF – which has a slightly less impeachable position in taking aim at the cause of the problem of child abuse – truly create a more secure environment for citizens is a matter of perspective on the issue of gun violence. However, it does seem clear that from Agamben's quote on the matter, Chicago likely is not engaging with all the potential causes of gun-related crime, which limits the security provided. Additionally, the power-dynamics created through the use of these programs represent a threat to another kind of security. If over-used, this technology has the potential to create a terrifying Panopticon-like scenario, or similar model where, instead of total visibility over all, a governmental policing system that focuses on only some types of crime or only some types of criminals. This not only has security implications, but implications regarding privacy as well.

4.2 Privacy

Coalescing with the theme of security is often the theme of privacy. Situated almost dichotomously within the debate on predictive analytics, the concepts of privacy and security stand seemingly opposed in the discussion of these programs and governance. In the creation of such databases and lists, put together by algorithms, the violation of the privacy of those on the lists (or with the potential to be on the list) is an important part of the discussion – as well as the broader discussion about the privacy of all citizens in an environment of anticipatory governance. This relationship represents a potentially monumental change in the relationship between the two, as the government has more access to more invasive technology than ever before in history – and its use of these programs is still relatively new and their long-term implications remain largely untested. Privacy is the glass that separates the constituents from the government and the use of such programs can either clean the glass for a more transparent relationship or it could shatter it.

The public reaction and the reaction from organizations like the ACLU show that the privacy invasion to those on the list caused by the SSL is not unanimously accepted as within the purview of the Illinois state government. In this, the SSL appears to represent a significant invasion of privacy and potential over-stepping of the bounds of government. Predictive analysis casts a shadow over certain members of society and may not be in line with the American legal presumption of innocence until guilt is proven in a court of law. Programs that anticipate crime

place those on the list they create somewhere between innocent and guilty – not quite either one. In the case of the SSL, status on the list also results in home visits that can disrupt the life and privacy of those being visited – based solely on statistics generated by a machine. Police visits due to these results move closer to something like the Panopticon – a seemingly dramatic comparison that becomes vastly more realistic considering the police's explicit explanation that the visits are designed to let subjects know they are being watched by the CPD, despite having committed no crime yet.

If Foucault's emphasis on the role of visibility in the Panopticon model is accepted, then these home visits represent a shift away, or even beyond, Bentham's vision of the model. In this way, the system created by the increase in governmental power almost becomes a focused not on everyone – the way a true model of the Panopticon implies – but instead on specific groups within its constituents who are being watched, observed, and critiqued more than others. While the creators of the SSL and RSF claim the technology eliminates biases based on race and gender, it has also been shown that algorithms can be programmed with prejudices or develop biases over time. Additionally, Like the location-based police programs like PredPol, this focus risks creating a statistical bias – certainly a group of people under police surveillance will seemingly commit more crimes than others who are not under police surveillance. In its purest form, the Panopticon does not anticipate, it only observes. By using the programs that anticipate crime, the Chicago state government and the CPD act more as the guard within the tower, perhaps only observing one row out of the many in their purview. In a world where those being observed are not actual prisoners, this is an unequal invasion of privacy as well as a less effective method. While the police focus on one row, what could be happening in the others?

The inequality of privacy created by the SSL and the RSF continues as any form of algorithmic regulation is also subject to biases – both planned into it through the algorithms and created by the data it produces. The SSL creator's promise that the algorithm lacks bias is not enough (Davey, 2016). Technology can contain flaws such as racial and economic biases and those cannot be overlooked – especially because removing things like race and gender in the case of the SSL also removes the data on who is most likely to be a victim of gun violence, an issue where those two characterizations can play a huge role especially in victimization – and, just like

in the discussion on security, fail to take into account societal issues that could account for the discrepancies.

The use of algorithms to create the SSL provides a glimpse into the debate around algorithmic regulation and governance as it showcases both sides of the security argument well. On one hand, this technology allows for government officials to have enhanced engagement in serious issues like gun control that have grown into rampant social issues with dangerous implications. If a government's role includes the protection of it citizenry, this aspect cannot be overlooked. In a modern world with ever-increasing access to technology – by both governments and criminals – can algorithms breach a gap between them? Does society's tolerance for these kinds of invasive programs chance as violence grows? Are these programs necessary in maintain safety in our modern world?

Much like the Panopticon, questions of both a moral and legal nature arise. The problem with posing these questions about the SSL is that to question police work is to question governance and to question governance is to question the very entity that decides what moral and legal considerations are taken into account in the creation of and adhering to the law. The shift mentioned by Foucault and Agamben, humans shift from 'object of' to 'subject of' government is seen here, as technology creates a greater disparity in power between the two. The central power of the government at the center figuratively towering over those it manages, the citizens, the 'subjects'. The further examine that relationship, it is necessary to look at the government-citizen relationship within the SSL and the RSF.

The shift from 'object of' to 'subject of' pointed out by Agamben is important in the discussion of the lists and databases created by these programs. Like Agamben and Foucault lament, over time, constituents of democratic governments have been shifted from the primary actor of governance to those that governance is acted upon. This shift means a decrease in power, which also results in a decrease in privacy. Submission to and compliance with such programs and databases requires relinquishing some privacy in order for the technology to function. In the case of the SSL and the RSF, being 'subject to' the government, and its law enforcement system, means adhering to the programs used by officials. In practice, those being put into these lists are not consulted beforehand nor have they given any form of consent to be placed on it. It is enacted upon them by a centralize power: the government. Governmental collection of personal

data is not new, but its use in these types of programs allows for focus on larger swaths of the population – or an even more focus on a smaller group of constituents – which has even greater implications.

4.3 Efficiency

In any debate about technology, efficiency is central to the discussion. A crucial tenant of technology is the role it plays in making more difficult tasks easier. The automatization of governance presents many issues, among them addressing whether or not it makes the government itself more efficient and how efficiently the technology utilizes is as well. To understand the efficiency of algorithms, it is necessary to have a greater understanding of what algorithms do with the information given to them. As aforementioned**,** algorithms are not static, they have the capability to adapt and react to the information feed into them, creating a process very similar to the way humans learn over time.

In 2016, a collaboration between Arizona State University, New America[13], and *Slate* produced a series entitled *Futurography*, the goal of which was to provide educational insight into the future of technology. One piece of the segment engaged with algorithms and their growing potential – and pitfalls – of technology featuring 'machine learning':

> When you ask a digital assistant, like Siri or Cortana, a question, algorithmic operations inform both its sense of what you've asked and the information it provides in response. Machine learning likewise helps Google Maps determine the best route from one location to another. And there's a virtually unlimited array of other functions that algorithms can serve: Some of the earliest commercial applications of algorithms involved automating tasks such as payroll management, but with the rise of contemporary machine learning, they're used for much more sophisticated tasks. Algorithms determine who should receive

[13] New America is a think-tank in Washington D.C. that focuses on public policy regarding technology, economics, education, and political reform. Their website states that it is an organization committed to "confronting the challenges caused by rapid technological and social change". (https://www.newamerica.org/our-story)

> government benefits, contribute to predictive policing, help anticipate health crises, reschedule airline flights, and much more. (Brogan, 2016)

The segment further delves into the mechanics of algorithms and what makes them so powerful in the modern world:

> "Generally speaking, when people talk about algorithms these days, they're talking about something more specific, like the operations that power our social media news feeds. In one way or another, most of these systems are examples of a technology called *machine learning*. Instead of repeatedly processing a stable set of instructions, systems based on machine learning rewrite themselves as they work. It's this that frightens some people, since it makes algorithms sound like they're alive, possibly even sentient. (To be clear, they are neither.)" (Brogan, 2016)

This 'machine learning' engages with a key part to of algorithms: their ability seemly to learn gives us greater confidence in them. It is perhaps due to this that they have given greater responsibility over the past decade. They can, in fact, get better at their jobs over time. However, this ability does not come with a learning curve:

> "Machine vision is an important example, since it also demonstrates the way algorithms often learn how to do their jobs better by messing them up, sometimes very publicly. Those errors can be silly, as when Wolfram Alpha mistakes a cute baby goat for a dog, but they can also be downright ugly, as when Google Photos misidentified two black people as gorillas. No one consciously taught the system to form racist conclusions, but the parameters that the programmers set up may have primed it to arrive there. Relying on machine learning is risky because these are systems that learn to get things right by repeatedly getting them wrong. Working with them therefore entails accepting almost inevitable errors and screw-ups." (Brogan, 2016)

This feature also notes that algorithms often feature more human interference than one might realize, maintaining the argument that, while algorithms cannot seem to master certain fields – such as customer service – humans and algorithms are not mutually exclusive (Brogan, 2016).

This outlook creates unlimited potential for the integration of the two in the near future, but the flaws inherent in this process must be emphasized.

However, programs like the RSF, work to integrate the algorithmic and the human to create greater efficiency. In the case of the RSF, efficiency is a big selling point for the company as the program potentially lessens the work load of social workers, who are often tasked with monitoring too many families and making critical decisions regarding the safety of at-risk child very quickly (Levenson, 2015). This is something at the forefront of the mind of Rhema Vaithianathan, a health economist at New Zealand's Auckland University of Technology, who is creating a model for Allegheny County in Pennsylvania. Vaithianathan spoke to the *Boston Globe* about how "haphazardly" child welfare employees decide which abuse reports and how algorithm-driven programs could provide more information to them so the would make the "best-informed decision" (Levenson, 2015).

The use of programs like the RSF offers an opportunity for a more streamlined approach to social work, a program that can 'look' for all the same identifiers as a human, but much faster. The human operator can then better use their time to focus on those with a higher risk assessment, better using resources across the board. Theoretically, the use of the program can increase the efficiency of the social worker and provide a safer – and more secure – environment for the child and family being monitored. However, that is only theoretically. In practice, the use of the RSF and programs like it creates issues of its own, including operator errors and misapplication. Even Vaithanathan admitted to the chance that if child welfare employees were given the "risk score", they may gain a false over-confidence in the results. On the issues, she said, "Humans like shortcuts, so when they see this number they might short-circuit their own professional judgment" (Levenson, 2015).

This issue is derived from several things, including the believe that algorithms are infallible, perfect systems that can somehow bypass prejudices and mistakes. Vaithianathan's use of the word "shortcuts" is important: if these kinds of programs are viewed as shortcuts to greater efficiency, they may be being misused. It has also been suggested that while these use of these programs does provide a way to more quickly identify children in danger, it also should require more steps within the social work field. The company that created and maintains the RSF,

Eckerd, has notes that caseworkers should not receive the raw scores and that decisions should not be made on the scores alone. The company recommends that the data be reviewed by supervisors who are trained by the Eckerd to use the identifiers and scores and identify the cases that are the most urgent (Jackson & Marx, 2017).

This format represents a way to integrate the program into the existing apparatus in a way that allow for greater oversight of the algorithm itself. The idea is, of course, that the algorithm will operate the same at a human social worker. The factors considered by the algorithm are based on factors that would be used by social workers to do the same work. These include the age of the parents, age of the child, history of neglect, whether the child was enrolled in day care, whether the parent had been a foster parent, history of drug abuse, and the presence of a boyfriend in the home (Levenson, 2015). All are factors that social worker consider in their work without the use of the program.

Presently, these programs and algorithms used for the identification of risk factors are only used on families and home that have been reported for abuse or neglect, in the same way that the SSL was only utilized on those arrested for previous crimes. However, to become a truly effective predictive model – in a way that it was not for Chicago, leading to the termination of its use in the city – some researchers say that the program would need to consider parents that have never been accused of abuse, "a fairly radical concept sure to trigger concerns about government overreach" (Levenson, 2015). The reasoning behind it is simple: the greater information given to the algorithm, the better it can to do its job. For example, if it was feed all information about everyone in a city, the algorithm could potentially identify child abuse (or the potential for child abuse) in homes that have never been reported. For issues that happen in the home and have strong power dynamics, like child abuse, that could be critical. In that case, a child being abused who was not in daycare or was too afraid to tell a teacher, would still be identified as at-risk. This would allow of social work departments to investigate cases of abuse that had previously gone unnoticed. However, the creation of a database like that would also implicate large swaths of society – young parents, former members of the foster care system, divorced parents – as "higher risk" without any evidence beyond previous statistics. This issue occurred in Chicago, when the over-identification of child in at-risk home and families, flood the system and actually decreasing overall efficiency in preventing child abuse (Jackson & Marx, 2017).

There is another component to the efficiency of the RSF program as well: the price tag. The program cost $366,000 to implement in Chicago alone (Jackson & Marx, 2017). The company, Eckerd, that developed the RSF, helps to run child welfare programs in Hillsborough County, Florida with a $73 million contract (Jackson & Marx, 2017). Predictive analytics are reported to be, in total, responsible for over $270 million worth in governmental programs and contracts worldwide (Jackson & Marx, 2017). Despite the heft of these initial investment, supporters of the program see it as a way to manage the increasingly scant resources of social work facilities and department around the nation. This is another potential advantage of algorithmic regulation: the long-term cost. Even if the algorithm comes with a high one-time price tag, it can quickly become a more attractive option than full salary and benefits for the numerous employees that make up governmental child services departments. Since its invention, the computer has represented the potential for automation of jobs and while the ethics are still hotly debated, the economics of this cannot be ignored. However, the monetary worth of these programs is contingent upon more than just the potential of efficiency. To offset the hefty initial investment, the programs must also work –and the effectivity of both of these programs has been contested.

4.4 Effectivity

The previous themes are all encompassed in the final theme: effectivity. Discussions surrounding security, privacy, and efficiency are all predicated on one central questions: How well do these programs work? Without knowing this, it can be difficult to know how much we, as a society, are willing to give up in exchange for the services provided by these algorithms in governance. After all, it is difficult to argue for the violation of privacy in exchange for increased security and increased efficiency if the program doing the work cannot complete its task well. In the analysis of effectivity of these programs, the very idea of anticipatory governance is questioned because, taken to an extreme, it leads us to the question: What happens when the Panopticon tower fails in its objective?

Since its introduction, the SSL has been met with both praise and resistance. Praise for the way it combats violence in an increasingly violent city, but harshly critiqued for its privacy invasion, its potential biases, and the mystery surrounding the algorithm itself and how it identifies those it places on the heat list. The algorithm's creator, professor at Illinois Institute for Technology, Dr.

Miles Wernick, has explained that the model "intentionally avoided using variables that could discriminate in some way, like race, gender, ethnicity and geography" (Davey, 2016). However, the CPD will not release the ten variables that do make up the model, citing proprietary technology. A New York Times article, however, reported examples from the CPD such as "Have you ever been shot?" or "Do you have an arrest for weapons?" (O'Connell, 2017). The exact mechanics of the current algorithm remain unknown – or at least, unreleased by the CPD – as the algorithm is constantly being updated. However, after a legal battle, the CPD was forced to release an older version.

After the Chicago Sun-Times requested the full list under the Illinois Freedom of Information Act in 2016, the CPD denied the request. However, after a lawsuit was filed, the office of the Illinois Attorney General, Lisa Madigan, found the CPD was violating the law by not releasing the information (Dumke & Main, 2017). In 2017, the City of Chicago then released the database from 2016, revealing CPD data from the previous four years, and including additional risk factors, such as age, narcotics or battery arrests, gang affiliation, and status as a victim of battery or shooting (Dumke & Main, 2017). Without additional information from the CPD, such as how much each factor is weighted, all analysis of the dataset is speculative. However, using a linear regression model, the New York Times was able to recreate many of the same responses and possibly identify the weight of the factors. The NYT's research found that the most significant factor seemed to be the person's status as a victim of battery (+34 score) and the least seemed to be age (-41 score). Gang affiliation ranked low among the available factors (+4 score), with "barely any impact on the score" (Asher & Arthur, 2017), combatting the common public perception that gangs are to blame for the majority of violence.

The release of this dataset has increased scrutiny of the CPD – and how they claim the SSL works and its effectiveness. As far as the CPD claims that violence was concentrated at the top of the list, the review of the dataset has mixed results:

> The top 1400 people have scored of 429 and up, and they are in fact disproportionately involved in violence. But that disproportionate share amounted to less than 20 percent of the total gun violence in Chicago in 2016…the Chicago Police Department declined to comment on the accuracy of Chief Johnson's statement. (Asher & Arthur, 2017)

Creator Wernick has commented that the algorithm has been updated since the release of the dataset, but those changes have not been made public, adding to concerns about legality and transparency (Asher & Arthur, 2017). Papachristos, whose research inspired the SSL, has since distanced himself from the program, citing the lack of transparency as well as the anticipatory nature of this kind of police work. Instead, his "work focuses on identifying potential victims, not on predicting the chances someone will shoot another person" (Main, 2017). This means the SSL is reaching further than the research it was initially based upon, creating more questions about the implications of its use by police.

Additionally, the effectivity of the RSF program has also been called into question based on the results it provided in Chicago. RSF and programs like it, exist in numerous states across the nation other than Illinois and Florida, including Massachusetts, Pennsylvania, Ohio, Indiana, Maine, Louisiana, Connecticut, Oklahoma, and Tennessee. However, Illinois recently discontinued its use of the RSF in late 2017, when officials in the Department of Children and Family Services (DCFS) found the service "unreliable" (Jackson & Marx, 2017). Instead of decreasing workloads, they were increased as more than four thousand children were given high-risk scored – or even statistically certain death within the upcoming years, as was the case with nearly four hundred children in the system (Jackson & Marx, 2017).

Despite these high numbers of house identified, however, the programs failed to identify several households as high-risk – and children in those homes died, resulting in criticism of both the department and the program. In Illinois' case, not only did the algorithm not increase efficiency in the allocation of department resources, it also failed in both its and the department's primary objective: keeping kids safe. As DCFS Director Beverly Walker put it later in an interview about why the program was discontinued: "We are not using the predictive analytics because it didn't seem to be predicting much" (Jackson & Marx, 2017). Like with most advances in technology, the algorithm was easy to defend when it was working and difficult when it was not, so Illinois removed the program.

Unsurprisingly, there is no a consensus on the effectivity of these programs overall. Discussion about the effectivity of these programs is often paired with a discussion about how the data generated by these programs should be used. The algorithm generates scores, but perhaps

another step should be placed between those scores and the social workers who make decisions based off them. The way the data is accessed is a critical issue as the programs remain in numerous states. Despite the outcome in Illinois, many of the programs' supporters point out the successes elsewhere. However, further research into those successes poses more questions. The company behind the RSF, Eckerd, cites the "remarkable" achievements of the program in Florida, which the company claims "virtually eliminated abuse-related deaths of wards in Hillsborough Country since 2012" (Jackson & Marx, 2017). However, reports made by the Chicago Tribune, found differently. Five children died while being monitored by the program between 2015 and 2016. Eckerd claims that four of these fatalities were not child-abuse related and were instead accidental deaths not under the purview of the program. However, one child's death has resulted in first-degree murder and aggravated child abuse charges for the foster family (Jackson & Marx, 2017). Eckerd's report did not account for this case. Similarly, Chicago's use of the program not only generated too many high-risk scores, it also failed to identify two cases that did result in the death of the child and resulted in high-profile failures for the department (Jackson & Marx, 2017).

4.5 Overall

The themes of security, privacy, efficiency, and effectivity offer a chance to consider the best and worst of what algorithmic regulation through programs like the SSL and the RSF has to offer. It is clear that technology has moved beyond a point that most governmental theory – including Agamben and Foucault over the past decades – could have anticipated directly, but the warnings in Agamben and Foucault's philosophies are coming true. The constituents' role contra the government has changed, with the constituent's power diminishing. In exchange, they are offered security and efficiency by the government, which may not actually be able to provide effective results or protect any provisions of privacy for the constituent while doing so. In the case of Chicago, it is the lack of effective results that was the downfall of their RSF program and drawing a more critical eye upon its use of predictive analytics throughout the Illinois state government and law enforcement.

It appears that a more comprehensive understanding of the effectivity of these programs – and what "success" looks like – is necessary, especially in the face of the serious criticism against them. There are a range of opinions about programs like these, especially regarding an issue like

child abuse. On one hand, this level of data-collection and algorithm use can be perceived as governmental overstepping – or even Orwellian. On the other hand, this technology provides a change to help identify and potentially prevent a crime that occurs inside homes and can be difficult and complicated for police to engage with or investigate. The push-back against this program by the Illinois government appears to be based in the ineffectively of the program's results – not the program itself. This begs the question: if programs like this were somehow guaranteed to work, would the public accept the government's usage of them? Should they?

The generation of these kinds of questions alone reveals that the relationship between the US government and its constituents has changed in response to the employment of algorithmic regulation. The use of programs like the SSL and the RSF, however, represents a tangible change in how governments interact with – or, more specifically, police – constituents and the reaction of the institutions like the ACLU reveals the presence of unease about such a change. Chicago's embrace of the SSL and rejection of the RSF reflects the tumultuous relationship possible between government and technology – and how the unease experienced by the public may have a firm basis if even the government finds the programs ineffectual. The power dynamics are shifted by the introduction of such technology and while growing pains are to be expected, they do not come at no cost to the relationship between the government and its constituents. A greater sense of unease is evident, along with a greater concern about the growing power – and potential power – of the government.

However, alongside these concerns about potential risk, are very real benefits and the undeniable ubiquity of technology in governance. The relationship has changed, is changing now, and will likely change much more and the only reasonable middle-ground appears to be the creation and adherence to a set of legal regulations for the use of algorithmic regulation. The lack of regulation in the area currently is a concern shared by many academics, researchers, and citizens, and it is a fair criticism that the government may be overstepping its traditional role in its use of algorithmic regulation and altering how it relates to its constituents through a one-sided increase in power.

Statistically, the effectivity of these programs in American policing is questionable, but even if the SSL and the RSF do not bring unanimously accepted quantifiable results, they may provide a sense of safety in response to societal threats like gun violence and child abuse. The use of these

kinds of programs – and the CPD and DCFS's comments about deterrence and predictive analysis support this – proves the trend into anticipatory governance at a level that simply could not have existed before. The negative response by organizations and citizens to the lack of algorithmic accountability, including the comparisons to science-fiction, reflects this change as well. Comparisons to the Panopticon – even the modified model created by governmental specific focuses – may be well-situated for the study of the power dynamics of a technology-based government, but the use of a prison model does assume one thing: that those on the outside are prisoners.

In this case, the term 'prisoner' can be flexed, not meaning a literal prisoner but rather one that is under the dominion of the state, perhaps under its total control. The US Constitution gives acknowledgement to the creation of a government by the people, driven by democracy where those being governed have control over who is doing the governing. This system relies upon a balance between these powers. However, certainly, what the use of this type of anticipatory and predictive technology does definitively is alter the balance between the power of the government and the power of the people. When the government's role shifts to anticipatory – as it does in the cases of the SSL and the RSF – it is what Agamben pointed out as the shift of a constituent from an *object of* governance to a *subject of* governance, a fundamental change in both the power and role of each party. This change means everything for the constituent, who now exist as something government is enacted upon – and by a government with rising technological power – and achieving a status, as Foucault and Agamben contended, of a "modern man is an animal whose politics calls his existence as a living being into question" (Agamben, 1995, p. 3).

The resistance against this change also reveals that as this governmental role is changing, perhaps the constituent's role should be changing as well. If the government's role shifts to anticipatory then the constituent's role needs to shift to anticipatory as well. This is best accomplished through regulation. Regulation offers a chance to anticipate and prevent overstepping by governmental departments and agencies. The use of this technology requires more regulation to maintain the balance between the relationship of the government and its constituents. This regulation is also necessary because the government's changing role is unavoidable. The government must adjust to be better prepared for newer threats. However, like Agamben critiques, the government should be focused on treating the source of the problem, not

only the effects. Emphasizing algorithm-driven programs like the SSL and the RSF attempts to stop crimes before they happen, but does nothing for changing the reasons – society, economic, or otherwise – behind why the crimes are going to be committed. In this, the government is ignoring what should be part of its role, if Agamben's assessment is accepted, and instead focusing efforts on something that will only treat part of the issue. All of the categories of security, privacy, efficiency, and effectivity could also be achieved or obtained through the use of strategies that focused on the sources of societal issues like gun violence and child abuse as well.

The use of algorithmic regulation by the Chicago Police Department and the Illinois Department of Children and Family Services has altered the power dynamic between the people of the city and the governmental offices they interact with, the shift favoring the government and its offices and agencies. As the use of these programs is not limited to the city of Chicago, this represents a shift in the power dynamics across the US where ever these programs, and others like them, are being utilized. These programs are indictive of a shift toward greater anticipatory governance which includes both potential benefits and risks. In exchange for diminishing power, constituents are theoretically to achieve greater security offered through governance, however it comes at cost of privacy. With the inconsistent effectiveness of the programs, the role of constituent is seemingly placed in a position to become anticipatory in nature as well and demand regulation for the technology being use against it, forcing a transition back to a status as an *object of* governance, the way Agamben contends constituent were formerly. Doing so would provide a necessary check on the power of the government, especially in a democratic governmental system like the US.

The risks of these programs are apparent – and the relationship between the government and the constituent must shift again to maintain and equilibrium of power – but the potential is just as clear, and too tempting for governments to ignore. Overall, the blend of risk and potential inherent in the program, as well as the relationship between those utilizing predictive analysis and those it is being used upon, can best be summed up in this quote from Vaithianathan: "Yes, it's Big Brother," Vaithianathan said. "But we have to have our eyes open to the potential of this model" (Levenson, 2015).

5. Discussion

The controversy around government and technology is a global one. Newer forms of technology have blurred national borders and jurisdictions. How governments contend with and utilize technology is an issue faced by every government around the world, it is not solely an American problem. This thesis has sought to engage with the relationship between the US government and its constituents, but the status of other nations is not irrelevant. In fact, the exploration of the issue is only enhanced by looking at another environment. To offer a contrast to the American case studies, recent updates to European Union laws regarding data collection and protection can be explored and questioned, as well as the global implications of regulating a formally border-less medium like the Internet.

On May 25, 2018 the European Union's newest data protection law, the General Data Protection Regulation (GDPR) went into effect, updating the previous EU Data Protection Directive 95/46/EC. The new legislation updates data protections in accordance to the increase of reliance on the Internet since EU Data Protection Directive 95/46/EC was enacted in 1995 (Data Protection: Rules for the protection of personal data inside and outside the EU, 2018). The GDPR requires increased transparency about personal data collection as well as solidifies the rights of EU citizens to protest collection and petition for the erasure of collected data. The GDPR is more comprehensive than its predecessor and represents a step towards greater citizen (or consumer) protection, but also faces criticism by those who believe compliance will be too difficult. Not only will businesses and organizations based in the EU be required to comply, but any businesses or organizations that interact with or within the EU will also be required to operate within the GDPR's parameters (Data Protection: Rules for the protection of personal data inside and outside the EU, 2018). The enacted of the law in May of 2018 was met with outcry from business. One *Forbes* article entitled "What to do if total GDPR compliance is impossible" cites the "fundamental tension between controlling data access and supporting innovation" (Schrock, 2018) and concludes that current technology limitations will affect how well

companies can comply. The author – an American, it perhaps should be noted – predicts, in fact, that most will not be able to comply with the new regulations.[14]

It is too early to tell the long-term effects of the introduction of the GDPR, but the diametric relationship between data protection and innovation presented does incapsulate the heart of the debate between business and organizations (including governments) collecting data and those whose data is being collected. Yeung, however, does not subscribe to the same dichotomy however, instead writing in an essay on EU data protection laws:

> "At a pragmatic level, the EU data protection regime (and basic data protection principles upon which it rests) was animated by a concern to strike an appropriate balance between the use of data and the protection of the interests of those to whom the data relate, in order to establish a set of agreed principles for handling personal data so that disparity in national standards would not impede the free flow of personal data across national borders and impede digital innovation." (Yeung, Making sense of the European data protection law tradition, 2017)

Taking departure in the history of data collection and its implication, Yeung instead focuses on the rights potentially violated by the collection and what regulation can do to curtail that invasion. This shift in viewpoint also reveals a difference between the European and American legal response to data collection.

There is a critical difference in US data protection laws versus EU data protection laws – in the US, largely, the laws are created within the states, not at the federal level. This means that within

[14] This prediction did ring true for several US-based publications, including the *Chicago Tribune,* which, in lieu of compliance with the new regulations, terminated European access to their websites following the GDPR rollout on May 25th, 2018. Attempts to access the Chicago Tribune's website from Copenhagen, Denmark on June 1st were met with this message: "Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism." By June 1st, the publication had not announced immediate plans for compliance with GDPR regulations or the reinstatement of European access.

the US, the laws regarding the protection of data, utilized by both private and public organizations, can be different in California than New York. This highlights a fundamental difference between the governance on the two continents as well as one of the key issues in creating regulation regarding algorithmic regulation in the US. The outcry over the EU and the GDPR – and how any one operating within or through the EU must comply – shows the potential backlash to the creation of strict federal law around algorithms in the US., where, as aforementioned, the tenth Amendment to the Constitution protects states' rights to legislate issues not mentioned in the document.

The GDPR gives – or attempts to give – rights about their data back to citizens and, as Yeung points out, brings the issue about the "social foundations of democratic orders" that the new legislation seeks "to safeguard" (Yeung, Making sense of the European data protection law tradition, 2017). In this case, if the rise of data and algorithms represents a governmental Panopticon, the legislation like the GDPR uses legal protections to elevate those on the periphery to more than prisoners.

The GDPR engages with data collection broadly, both publicly and privately, and is not specific to algorithmic regulation. But it does show the growing concern about the encroachment of technology onto citizens' rights as well as provides an example of a strong governmental response. However, there is one additional protection added by the GDPR that bears particular importance to the discussion on algorithmic regulation. On the European Commission website, under the headline "What are my rights?", the following is listed:

> "You have the right to…request that decisions based on **automated processing** concerning you or significantly affecting you and based on your personal data are made by natural persons, not only by computers. You also have the right in this case to express your point of view and to contest the decision." (Data Protection: Rules for the protection of personal data inside and outside the EU, 2018)

This specification of automated processing – placed in bold on the website – highlights an important issue in algorithmic regulation: when processes that were formerly completed by humans instead become automated. The concerns about this issue have been forecasted in science-fiction books and movies for decades, but in modern society they are both theoretical

and practical as algorithmic regulation becomes increasingly widespread, powerful, and accepted.

The question of how humanity fits into this debate is either on the outskirts or at the very center. It is a question that has plagued theorists and academics for decades: Can technology become human? Given advances in artificial intelligence, this question only grows more and more relevant in today's world. What separates us from our technology? If technology can pass Alan Turing's famous test, does that affect how it should be treated? Does it affect what role it should play in governance? What if we modify the Turning test for algorithmic regulation and introduce this argument: Any humans performing a task have a failure/error rate so if an algorithm is able to perform the same task with the same failure/error rate, would having that algorithm perform the task have any *functional* difference? Quantitatively? Qualitatively? Certainly, just because an algorithm *can* perform a task at the same rate does not mean that it *should*, but it still an issue worth exploring.

The relationship between governments and citizens explored throughout this thesis is predicated upon human beings being the central players and employees. However, the scope can be expanded to include more types of technology to test the governmental theories further. Is the controversy around algorithmic regulation the use the computers in general? Or the (even potential) failure rate they may achieve? If it had a one hundred percent success rate, would it matter? What if it has the same failure rate as a human being? What would be the difference? Who decides that?

To explore this, let us assume the existence of an algorithm with the exact same failure rate as a human[15] and imagine it in the role of a governmental employee. The algorithm is tasked with assignment X, which it completes successfully 90% of the time – the same as the former employee completing the same task. Theoretically, there is no difference between the two. The controversy seems to surround just what assignment X entails. When placed in the position of

[15] The Turing test is typically applied to robots, which would also be relevant, however has been slightly modified for use with an algorithm. If the point of the Turing test is that the participant does not know that they are interacting with a robot, in the case of algorithmic regulation – where physical appearance, personality, and social aspects are not relevant – the most critical feature is the failure rate, the only measurable way to study success.

doing a task performed exclusively by automation, such as changing red traffic lights to green traffics lights, the risk of danger is extremely low. If the algorithm does not perform well, the worst-case scenario is that traffic moves slowly which would be frustrating, but not fatal. In this case, it would seem ridiculous to have a human doing the same job, even if the failure rate was the same. However, the decision to change from a red light to a green one is not complex and requires little assessment. What about a decision with more at stake and with more variables? Could the use of the algorithm be defended then? A math equation getting green lights patterns 90% of the time seems okay, but what about taking emergency response calls? Driving an ambulance? Piloting drones and bombers?

While the nuanced technology necessary for these types of roles may not exist currently, it is closer than it seems. Google recently introduced new features for its Assistant program that include the ability for the artificially intelligent assistant to place calls for the user (Google Assistant to make phone calls for owners, 2018). The official roll-out of the update featured a phone call with the Assistant in which the AI is nearly unrecognizable as a computer. It uses natural pauses, filler words, and reacts quickly to changes introduced by the other side. In the example, the program calls a hair salon to make an appointment for noon. However, the employee at the salon informs the Assistant that the closest time is at one-fifteen. The Assistant does not immediately take the closest time, but instead responds by asking about earlier times, per the instructions given to it by the user before the call was placed. This example phone call – along with one other that was made during the demonstration by Google chief executive Sundar Pichai– were debuted to reveal the realistic new AI powering the program (Google Assistant to make phone calls for owners, 2018). The conversation tone makes it different to identify the AI, meaning the person on the other end may not realize they are interacting with a computer, however, it is the ability to respond and make decisions that sets this technology apart. It is this aspect that technology has been missing, making it incapable of other governmental jobs. If the technology continues to advance in this direction, it will become a very real possibility that it could find its way into governance.

The potential for algorithmic regulation paired with these advancing technologies forecasts a future with even more complexities between technology and governance. Foucault wrote about the government's ability to decide who was human and who was not– a notion may take on a

new, more literal sentiment soon as AI advances enter further. As companies gain greater access to such technology, there is more reason than ever to re-evaluate the role of government and technology in a modern society and create more concrete regulation surrounding the way the two intertwine. Our understanding of algorithmic regulation as a society has increased over the past decades, but we will have to continue to advance our understanding of the technology around us, especially as it begins to seem less like technology and appear, sound, act, and think more like a human.

6. Conclusion

It is clear that the introduction and utilization of algorithmic regulation, including programs like the SSL and RSF, has had an effect on the relationship between the US government in Chicago and the constituents. Its role in daily life – in police work, social work, and beyond – has implications for its use around the country and the globe, as it shifts governance into a more anticipatory role and subsequently grants the government more power over the constituent. In order to create a new equilibrium, constituents – and organization and institutions run by constituents – must respond with anticipatory measures of their own in the form of regulation on how governments at both the state and federal level can utilize all forms of algorithmic regulation.

In studying this relationship, first, governmental theory was explored through the philosophies of Agamben and Foucault. These philosophies established governance as a changeable format and delved into how the governmental role has changed over time, including an emphasis on whether the government focuses on causes or effects in their governance. Foucault's presentation of the Panopticon as a power structure was also utilized as a method of gaging and critiquing the shift of power that can accompany governmental role changes. These philosophies paired with the STS concept, the identified modern governmental trend of anticipatory governance. This shift to anticipatory governance is supported both by Agamben's assessment of an effect-focused modern government that risks ignoring the causes, as well as Foucault's analysis of changing power dynamics.

Next, to provide a contextual framework for these theories, historical and technical background information was supplied about algorithms and their use in society since the mid-twentieth century. The broad term of 'algorithm' was more deeply explored as well as the varying applications and uses for them in society in the past half century. Public awareness of the technology has been limited – but growing in the decades since algorithmic regulation was first introduced and facing increasing criticism and opposition as the technology grows more and more powerful. Context for American governmental history and positioning was also supplied before the introduction of the two case studies of the SSL and the RSF in Chicago, Illinois. These case studies are examples of one ongoing use of algorithmic regulation and one program that was terminated.

Through a theoretical analysis of these case studies, the way changes in the governmental role affect its relationship with constituents can be seen and established through the use of four central themes of security, privacy, efficiency, and effectivity. These themes are most prominent in the discussions surrounding the application of the controversial technology and reflect both the praises and concern over the use of algorithmic regulation and predictive analysis. In looking at security and privacy, the shift from the constituents as an 'object of' governance, to a 'subject of' governance becomes clear as well as the inconsistent application of the technology across all members of a society – presenting a greater threat to some than others. Analysis of the efficiency and effectivity of the programs also revealed that the programs have inconsistent results and there is not one standard view of what "success" looks like in their application. This further complicates the relationship by dividing the populace over the results and continuing the controversy surrounding the use of such technology.

These case studies provide a glimpse into algorithmic regulation in the US yet are limited in only analyzing one city in one geographical area of the US – and the project is limited in only studying one nation. Algorithmic regulation is a global issue that deserves more attention as it becomes more and more entrenched in both our social and political lives. The European Union's new GDPR policy indicates a new trend in creating more protections for individuals versus technology – but its international backlash reminds us that, globally, technology is complicated issue with no concrete borders and jurisdictions. Regulating new technology will not be easy, however, it is certainly worth trying. Technological security and innovation are not diametrically opposed, despite arguments to the contrary – but do need to be explored further to create a safer future. New technologies, like Google's new Assistant, offer a glimpse into the continuing future of more advanced technology, the role of which has unlimited potential and an increasingly blurred line between technology and humanity.

Algorithmic regulation has massive implications in the future and how it affects global politics is an issue that deserves further study in the field of Global Studies. How such drastic shifts in technology and the potential power created by these technologies affect individuals in a town, city, nation, or around the world must be critically understood as technology continues to advance and entrench into society. As these case studies and analysis have shown, the relationship between the US government and its constituents is changing as the use of

algorithmic regulation increases, with greater power going to the governmental side as the individual constituent moves further from an ‘object of’ governance toward a ‘subject of’ governance. If an equilibrium is to be achieved and maintained, constituents around the world must know of their diminishing position and be given the opportunity to act.

Like Jackson’s Leviathan, algorithmic regulation is a tricky beast that accrues public favor when it is working and outrage when it does not. The very use of algorithmic regulation represents a drastic shift in how governments have operated historically and a change in the power dynamics at play in their relationships to their constituents. The modern trend of anticipatory governance coupled with the use of predictive analytics has the potential to create a monster of its own – one powerful enough to combat societal issues previously unsolved or one that summarily victimizes those it seeks to protect.

Bibliography

Agamben, G. (1995). *Homo Sacre: Sovereign Power and Bare Life.*

Asher, J., & Arthur, R. (2017, June 13). *Inside the Algorithm That Tries to Predict Gun Violence in Chicago*. Retrieved from The New York Times: https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html

Benbouzid, D. D. (2017). Evaluating predictive algorithms. In B. B. Leighton Andrews, *Algorithmic Regulation* (pp. 13-18). London: London School of Economic and Political Science.

Blatter, J., & Haverland, M. (2012). *Design Case Studies: Explantory Approaches to Small-N Research.* Palgrave Macmillan.

Brogan, J. (2016, February 2). *What's the Deal with Algorithms*. Retrieved from Slate: http://www.slate.com/articles/technology/future_tense/2016/02/what_is_an_algorithm_an_explainer.html

Chicago Police Department. (2016). *Strategic Subject List.* Chicago: The City of Chicago.

Cook, K. (2017). *Government and Technology.*

Data Protection: Rules for the protection of personal data inside and outside the EU. (2018). Retrieved from European Comission: https://ec.europa.eu/info/law/law-topic/data-protection_en

Davey, M. (2016, May 23). *Chicago Police Try to Predict Who May Shoot or Be Shot*. Retrieved from The New York Times: https://www.nytimes.com/2016/05/24/us/armed-with-data-chicago-police-try-to-predict-who-may-shoot-or-be-shot.html

Domingos, P. (2015). *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World.* Basic Books.

Dumke, M., & Main, F. (2017, May 18). *A look inside the watch list Chciago police fought to keep secret*. Retrieved from The Chicago Sun Times: https://chicago.suntimes.com/news/what-gets-people-on-watch-list-chicago-police-fought-to-keep-secret-watchdogs/

Fessenden, F., & Park, H. (2016, May 16). *Chicago's Murder Problem*. Retrieved from The New York Times: https://www.nytimes.com/interactive/2016/05/18/us/chicago-murder-problem.html

Foucault, M. (1977). *Discipline and Punish.* Pantheon Books.

Google Assistant to make phone calls for owners. (2018, May 8). Retrieved from BBC: http://www.bbc.com/news/technology-44045424

Gorner, J. (2016, July 22). *With violence up, Chicago police focus on a list of likeliest to kill, be killed*. Retrieved from Chicago Tribune: http://www.chicagotribune.com/news/ct-chicago-police-violence-strategy-met-20160722-story.html

Guston, D. H. (2014). Understanding anticipatory governance. *Social Studies of Science*, 218-242.

Hurley, D. (2018, January 2). *Can an Algorithm Tell When Kids Are In Danger?* Retrieved from The New York Times Magazine: https://www.nytimes.com/2018/01/02/magazine/can-an-algorithm-tell-when-kids-are-in-danger.html

Jackson, D., & Marx, G. (2017, December 6). *Data mining program designed to predict child abuse proves unreliable, DCFS says*. Retrieved from Chicago Tribune: http://www.chicagotribune.com/news/watchdog/ct-dcfs-eckerd-met-20171206-story.html

Jackson, R. (2007). *Sovereignty: The Evolution of an Idea.* Polity Press.

Levenson, M. (2015, November 7). *Can analytics help fix the DCF?* Retrieved from The Boston Globe: https://www.bostonglobe.com/2015/11/07/childwelfare-bostonglobe-com/AZ2kZ7ziiP8cBMOite2KKP/story.html

Lodge, M., & Mennicken, A. (2017). The importantance of regulation of and by algorithm. In L. Andrews, B. Benbouzid, J. Brice, L. A. Bygrave, D. Demortain, A. Griffiths, . . . K. Yeung, *Algorithmic Regulation* (pp. 2-7). London: London School of Economics and Political Science.

Main, M. D. (2017, May 18). *A look inside the watch list Chicago police fought to keep secret*. Retrieved from Chicago Sun Times: https://chicago.suntimes.com/chicago-news/what-gets-people-on-watch-list-chicago-police-fought-to-keep-secret-watchdogs/

Morozov, E. (2014, July 20). *The rise of data and the death of politics*. Retrieved from The Guardian: https://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation?INTCMP=sfl

Nelson, L. (2017, June 30). *Trump says he's sending feds to Chicago to hlep with crime problem*. Retrieved from Politico: https://www.politico.com/story/2017/06/30/donald-trump-chicago-crime-federal-help-240131

O'Connell, P. (2017, January 27). *Chicago police announce expanded technology to curb shootings*. Retrieved from Chicago Tribune: http://www.chicagotribune.com/news/local/breaking/ct-chicago-police-shotspotter-technology-met-20170127-story.html

O'Neil, C. (2016). *Weapons of Math Destruction.* Penguin Books, Limited.

Palmer, S. (2014, July 7). *7 hottest tech trends in 1776*. Retrieved from The Huffington Post: https://www.huffingtonpost.com/shelly-palmer/7-hottest-tech-trends-in_b_5564126.html

Romanyshyn, Y. (2017, September 26). *Chicago homicide rate compared: Most big cities don't recover from spikes right away*. Retrieved from Chicago Tribune: http://www.chicagotribune.com/news/data/ct-homicide-spikes-comparison-htmlstory.html

Sanahuja, L. C., & Ghia, F. (2015). *Cosmopolitanism: Between Ideals and Reality.* Cambridge: Cambridge Scholars Publishing.

Schrock, E. (2018, May 14). *What To Do If Total GDPR Compliance Is Impossible*. Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2018/05/14/what-to-do-if-total-gdpr-compliance-is-impossible/#3cfa42fc4da3

Sorkin, A. (1999). *Mr Willis From Ohio*. Retrieved from West Wing Transcripts: http://www.westwingtranscripts.com/search.php?flag=getTranscript&id=6

Sweeney, A., Schmadeke, S., & Meisner, J. (2017, January 1). *How to stop guns, gangs and poverty? Chicago seeks solutions after violent 2016*. Retrieved from Chicago Tribune: http://www.chicagotribune.com/news/ct-chicago-violence-solutions-met-20161230-story.html

US National Archives. (2018). *The Constitution of the United States: A Transcription*. Retrieved from National Archives: https://www.archives.gov/founding-docs/constitution-transcript

Yeung, K. (2017). Algorithmic regulation: A critical interrogation. *ResearchGate*.

Yeung, K. (2017). Making sense of the European data protection law tradition. In B. B. Leighton Andrews, *Algorithmic Regulation* (pp. 34-44). London: London School of Economic and Political Science.