2021

Big Data as a Technology of Power

John Reynolds

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Big Data as a Technology of Power

John Reynolds

Supervisors:
Dr. David Neil
Dr. Patrick McGivern

This thesis is presented as part of the requirement for the conferral of the degree:
Doctor of Philosophy

This research has been conducted with the support of the Australian Government Research Training Program Scholarship

University of Wollongong
School of Humanities and Social Enquiry

January 2021

Abstract

The growing importance of big data in contemporary society raises significant and urgent ethical questions. In the academic literature and in the media, the dominant response to many of these ethical questions is to re-examine the role and importance of privacy protections, but I argue that it is far more fruitful to investigate the relationship between power and big data. As algorithmic processes are increasingly used in decision-making processes, it is crucial that we understand the ways in which big data can be used as a technology of power. Only then can we properly understand the ways in which the use of big data impacts on and reorganises society, and go on to develop effective, tailored protections for individuals against harm from the use of big data. First, I show that the rise of big data highlights the limits of privacy protections, as big data-based analytics allow for personal information to be inferred in ways that circumvent privacy protections and problematises the category of personal information. In order to properly protect people from the potential harms that can arise from the use of big data in decision making, I argue that we must also examine the relationship between big data and power. In this thesis, I will present an argument for a pluralistic understanding of power, and a lens through which we can identify the kinds of power being exercised in the contexts we are investigating. Power is best understood as an umbrella term that refers to a diverse range of phenomena across an equally diverse range of domains or contexts. We can use this attitude to examine the central features of an exercise of power to identify the relevant theoretical accounts of power to draw on in understanding the modes of power present in a context. In Chapter 4, I will demonstrate the value of this approach by using it to analyse four contexts where big data is used as a technology of power, showing that we cannot use a single theoretical understanding of power across all exercises of power. Following this, I examine the impacts of big data on the operation of power. While many in the literature see big data as necessitating the development of new theoretical understandings of power, I argue that there are important historical continuities in power. Big data can be picked up and used as part of existing kinds of power just as any new technology can, and while this may change the efficiency, range, and effectiveness of exercises of power, it does not change their fundamental nature. However, there are impacts on the operation of power that are unique to big data, and one of these impacts I consider here is that the inferential capabilities of big data shift power from acting on human subjects and towards acting on data doubles (fragmentary digital representations of people). This leads to significant ethical problems with ensuring that power is exercised accountably. Finally, I will demonstrate these problems in Chapter 7 through examining four more contexts in which big data is used as a technology of power, showing how the shift to the data double as the subject of power undermines the effectiveness of accountability as a check on the abuse of power.

Acknowledgments

I acknowledge the Traditional Custodians of the lands on which I have researched and written, and I pay my respects to the Elders past, present, and emerging. My research has been performed on the soil of the D'harawal Nation, and I acknowledge the spiritual and cultural connection between the D'harawal Nation and Country.

Despite my native introvert tendencies, the process of writing this thesis has in many ways been a collaborative one, and there is a list of people whose contributions must be acknowledged. While I have tried to include everyone, it is likely that I have forgotten someone, and if that is the case, I offer my sincere apologies and deep gratitude.

First and foremost, I am deeply indebted to my supervisors, David Neil and Patrick McGivern. David, as my primary supervisor for both my honours and my doctoral theses, I am so incredibly grateful for your guidance and assistance over the last five years. While I have always been interested in both the ethical use of technology and the nature of power, you helped me find a way to express those ideas together and find a way to investigate and explain those interests. Thank you for everything, particularly over this crazy 2020. Patrick, your added assistance has been invaluable, and I am so grateful. Thank you for your fresh eyes on drafts from time to time, but more importantly for your support and your assurances that my plans are achievable. I am incredibly lucky to have had both of you on board in this project, and I will always be grateful.

I would be remiss to not mention those who tutored me as part of my undergraduate degree at the University of Wollongong. When I started university, with very little idea of what I wanted to do with my degree, the philosophy program was there as a place to explore big ideas and new concepts, that challenged my thinking and helped me find something I was passionate about. In particular, I need to thank Michael Kirchhoff for his engaging teaching style, and Sarah Sorial, who did so much to inspire my passion for philosophy.

A huge thank you also needs to be extended to a long list of friends, and I cannot list everyone by name here, but I will try my best. Firstly, to my fellow graduate students at the University, the discussions I had with you in the early stages of my writing were incredibly helpful, particularly one work in progress presentation that helped me cement the contents of Chapter 2. Secondly, my work family at Specsavers, for being so understanding with scheduling, and always finding a way to cheer me up with laughter. Thirdly, to the long list of friends I have met through community theatre, including Gillian, Jason, Amy and the rest of the Copeland family, Jesse, Connor, and Nathan. Theatre has in many ways been an escape from studies for me, so thank you for your friendship and support through life. Fourthly, thank you to Sam for always being around for a deep conversation about any and every philosophical topic, and apologies for always promising to send you drafts to read and forgetting to do so. Finally, a thank you to Suzi, for your friendship over the last few years, and an apology for possibly inspiring you to undertake the same mammoth task that I have.

Thank you as well to my family who have been so incredibly supportive of me and my studies. My cousin Charlotte, for your love and support I have been changed for good. My sister Stephanie, thank you for the practical advice around job hunting for after the thesis, and being a wonderful sister. I am lucky to have you. And of course, Mum and Dad, Julie and David. You have both been such huge inspirations for me, and to properly thank you for everything would require a whole acknowledgements section in and of itself. Thank you for your support and unwavering belief and thank you as well Dad for the help with editing.

Now for my amazingly supportive husband Troy. Thank you for coming on this journey with me, whether you wanted to or not. Thank you for the support, the assistance, and the love you gave me over the course of this project. Thank you for every now and then reminding me that I can do it, but that perhaps I should try again tomorrow after a break. I cannot apologise enough for putting you through a year of thesis writing and wedding planning, but you stuck by me and helped me through it all.

And finally, to Saffy and Quentin. It is often easier to get through the loneliness of writing with a cat on your lap and a string to chase.

Certification

I, John Reynolds, declare that this thesis submitted in fulfilment of the requirements for the conferral of the degree Doctor of Philosophy, from the University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. This document has not been submitted for qualificationsatanyother academicinstitution.

____

John Reynolds

7th January 2021

Table of Contents

Chapter 1

Introduction

We are now well and truly living in the age of data. Data has become the foundational building block of governance and a primary economic resource. Governments and public bodies are using big data to track everything from citizens (Raphael & Xi 2019) to the spread of diseases (Jin & McGorman 2020; Lazer et al. 2014), while law enforcement agencies are using big data to identify suspects (Asaro 2019; Mann & Smith 2017) and secure convictions (Kirkpatrick 2017). Big data drives our smart cities (Picon 2015), our cars (Stilgoe 2018), and our online interactions (Bozdag 2013). Private companies are using deluges of data to track consumers to advertise to them (Boerman et al. 2017) and employees to micro-manage them (Ajunwa et al. 2016; Perryer et al. 2016). Big data tells us what to watch (First 2018), what to wear (Zhou et al. 2017), what to eat (Holmes 2017), and someday soon may tell us where to work and who to marry (First 2018). Big data has become ubiquitous across society, and everyone feels its impact.

Proponents of big data claim that big data is the only solution, or at least will play a huge part in solving huge societal problems, such as halting climate change (van Rijmenam 2019) or stopping the spread of major diseases like dengue or influenza (Del Valle 2019). Others suggest that without the use of big data, cities in the future will become unliveable. Some estimates suggest that by 2100 over 80% of the human population will live in cities, and the only way this will be workable is by embracing big data and transforming all of our cities into smart cities (Wright 2018). While there are many who are excited by the changes that big data is bringing about, there are also many others who are pessimistic about the development of big data. There are very real concerns that the widespread use of big data will lead us to a dystopian future, where big data will be used to spy on people and supress individuality (Botsman 2017). Even some who work in the technology industry are now voicing concerns about the disastrous impacts of big data on a wide range of human life (Lewis 2017), from lowering our IQ scores and capacity to concentrate, to the destabilising or even dismantling of democracy itself.

A central assumption within this debate over whether big data will solve all our problems or doom us all is that it is a revolutionary technology, and that the world will never be the same again. However, I contend that it is important to step back and look past the Panglossian or doomsayer rhetoric and try to better understand exactly how the development of big data transforms society. The purpose of this thesis then is a kind of framing exercise for understanding the ethical implications of the impact of big data on society. To bring into focus the ethical consequences of big data it is necessary to examine the ways in which big data is used in the exercise of power.

In answering these questions, I agree with the suggestion made by Mayer-Schönberger and Cukier (2013, p. 141) that 'the biggest impact of big data will be that data-driven decisions are poised to augment or overrule human judgment.' Big data is increasingly being used in decision-making processes, and not just as a tool to aid decision making. Many decisions are now being routinely made through partially or fully automated processes. Companies such as Amazon are using big data to automate decisions on who to hire (O'Neil 2016) and who to fire (Tangermann 2019), while the Chinese government is using big data to deny citizens access to air travel, high-speed rail, and visa applications through automated processes (You 2018). Police forces are using automated facial recognition processes to track and identify suspects (Brey 2004) as well as algorithms designed to predict individuals who are likely to commit offences (Griffard 2019). While judges still have the final say over bail conditions and criminal sentences, several jurisdictions in the US are now using big data to generate risk scores for defendants, semi-automating judicial decision making (Angwin et al. 2016). As these decision-making processes become driven by automated processes that utilise big data, they are changing in ethically significant ways.

These changes in decision-making processes are the focus of this thesis. I contend that in order to properly understand the ethical implications of the use of big data in decision-making processes, we must understand the ways in which big data can be used as a technology of power and how the use of big data changes the operation of power. For example, we can see that the changes in decision making lead to a change in our understanding and experience of authority, both in the sense of authority as a person with expertise in a subject area and authority as the right to make binding decisions.

First, in the sense that a person with authority is a person with subject expertise, the use of big data is increasingly supplementing or even ‘replacing’ authorities. Algorithmic processes that utilise big data can make use of volumes of data that humans cannot naturally process and can discover patterns and correlations that would otherwise be invisible. In many areas, this ability to detect patterns and correlations is increasingly more useful than the expertise of traditional knowledge authorities, including in decision making processes. Algorithms for writing and curating news stories are replacing human news editors; as educational content is generated and delivered automatically, the role of human educators is being altered; as products are recommended algorithmically, we no longer need to rely on professional reviewers (Mayer-Schönberger & Cukier 2013, p. 141). This is not to say that big data is necessarily superior to human expertise, nor that human expertise can indeed be entirely replaced with machine learning. But in many areas, big data is increasingly taking over the role of traditional knowledge authorities in decision making processes.

Second, the nature of authority is altered. Someone who holds a position of authority in a power structure typically has the right to make certain binding decision and bears responsibility for those decisions. Authority may be vested in persons as a kind of personal authority, seen in the relationship between parent and child or teacher and student, or it can be vested in offices as official authority, such as in the hierarchical offices of a company or public institution (Arendt 1986, p. 65). However, as big data is used in the algorithmic processes that are increasingly automating decision making, human authority is ceded to those algorithms. Where decisions are made by an algorithm, it is unclear what happens to the authority vested in a person or in an office who previously made those decisions. We do not yet have an adequate understanding of the effects automated decision making will have on conceptions of authority and responsibility.

To understand these changes in authority, and other impacts on the operation of power, that come from the use of big data in decision-making processes, it is essential that we understand the ways in which big data is used as part of exercises of power, and how its use changes those exercises of power. There are a growing number of writers in the academic literature who are also considering this same point, such as Cheney-Lippold (2011), Rouvroy (2016; 2013), Thompson (2016), Beer (2016), Matzner (2017), Han (2017), and Zuboff (2019). Some authors, such as Rouvroy (2016; 2013), Beer (2016), Han (2017), and Zuboff (2019) argue that the development of big data has led to a dramatic transformation in the nature of power, and that we must develop an account of "data power" – a new theory of power for the digital age. While it is true that digital technology has changed the operation of power in many ways, it is important not to construe a new technology of power as somehow constituting a new *kind* of power. To properly address important questions of what effect big data technologies have on the ways that power is exercised by governments, corporations, employers and institutions, we need a more nuanced understanding of the relationship between big data and power, and this in turn requires us to pay attention to the variety of forms of power.

To this end, I will argue in this thesis that in order to understand the relationship between big data and power, we must adopt a pluralistic conception of power. By a pluralistic conception, I mean that we should be sceptical of the idea that it is possible to develop a single overarching and unified theory of power. We use the word power to refer to a diverse range of phenomena, in a similarly diverse range of contexts. Notions of "power" are applied at vastly different scales, in contexts as small as family relationships and as large as the manoeuvres of nation-states in international diplomacy, and are applied across a diverse range of domains, for example economics, the judicial system, schools, and so on. Instead of attempting to develop a single theoretical account that explains the relationship between big data and power, adopting a pluralistic attitude allows us to identify the conceptual features of different kinds or forms of power at play within a given context. This allows us to develop a nuanced and contextualised understanding of power, which directs our attention to the specific ways that big data technologies are used in different contexts.

Importantly, this approach to power allows us to understand the key features of big data that leads to its revolutionary impact on power within the specific contexts we are studying. Big data is a revolutionary technology, but there are still important historical continuities in the operation of power post and pre big data. Big data, like any other new technology, will alter the operation of power, such as by making exercises of power more efficient, by increasing the range that power can operate at, or by increasing the effectiveness or force of power. However, the use of big data does not inherently lead to a totally new kind or form of power. Instead, it is the unique inferential capabilities of many big data technologies that lead to its revolutionary impact on the operation of power, namely that the use of big data shifts power away from targeting people and towards targeting data doubles.

The data double, as I define it in this thesis, are digital representations of an individual that both contain and enable inferences about an individual. Data doubles are constructed from fragments of data about an individual through data-driven surveillance, or dataveillance (Haggerty & Ericson 2000, p. 613). These digital representations can then be used to categorise and identify individuals, but they also contain predictions and enable the making of further predictions about a person's future behaviour. Exercises of power can then target data doubles as the subject of power, both in the sense that they can be targeted as a kind of shorthand to target a specific individual, but also targeted as an entity in and of themselves. This is an important shift in the operation of power, which can be seen by avoiding overstating the impact of big data.

By picking out the ways in which big data is used in exercises of power, and how it impacts on how power functions, we can then understand the ways in which the use of big data impacts on our social norms and legal, political, and economic institutions. One important impact considered in this thesis is that it is increasingly difficult to ensure that power is exercised in ways that can be held accountable. As power shifts towards targeting data doubles, it becomes difficult to monitor the operation of power and objectively assess its accuracy and appropriateness, difficult to challenge through the imposition of sanctions as power gains a veneer of objectivity through its reliance on big data, and difficult to justify as decision-making processes become 'black boxed' and opaque even to those who exercise it.

The broad overview of this thesis is as follows. First, I will argue that existing approaches to the ethics of big data, which are based on the concept of privacy, can no longer fully cope with the ways in which big data operates. Instead, we should focus on the relationship between big data and power as a more fruitful foundation for legal and ethical protections for individuals against possible harms. To do so, it is necessary to set out a theoretical lens through which we can analyse the operation of power within a given context or example of the use of big data. This approach draws on a pluralistic attitude towards power, whereby we recognise that there are different kinds or "modes of power" operating in different contexts. To properly understand the operation of power within a given context it is necessary to be attentive to various contextual features as a guide to identifying the important conceptual features. But before providing a more detailed overview of each chapter, it is important first to briefly set out what I mean when I refer to "big data", as well as identifying some of the harms that individuals can suffer as a result of the use of big data.

What is Big Data?

There is no comprehensive and commonly accepted definition of the term big data, but I am not looking to set out such a definition nor to select one from the literature to work with. Instead, I am using the term big data broadly, to refer to the technological capability to perform analysis on large, often unstructured, data sets, the mindset or mentality of using data to find correlations and novel insights that can be used to make predictions, and the automated algorithmic analysis and decision making capacity enabled by the use of big data. The ways in which big data can be used can then lead to potential harms for individuals. There are many potential ways in which individuals can be harmed, but the two main types of harms that I am concerned with here are unjust discrimination and the undermining or limiting of autonomy.

The term big data is a kind of umbrella term that covers a variety of technologies, tools, and capabilities. In practice, the term big data is used as a kind of catch all term for a wide range of technologies including artificial intelligence, machine learning, predictive and prescriptive analytics, blockchain technologies, knowledge discovery and data mining tools, and also refers to the databases used as part of these technologies and to the tools used to collect raw data. As the focus of this thesis is on the use of big data technologies in decision making processes, there are two primary implementations of big data that are of particular concern, namely AI and machine learning. Modern AI is driven by big data, and AI systems such as automated computer assistants and self-driving cars are reliant on the use of big data to recognise speech patterns or driving conditions and provide coherent information and make decisions on how to drive. Machine learning, a type of AI, involves the training of algorithms using statistical methods to detect patterns and make decisions. These two technologies are of most concern here because of their increasing use in decision making, and the ethical impacts of their use.

Beyond the myriad technologies that make up big data, those technologies are then used in a diverse range of domains, spanning economics, politics, the judicial system, international relations, culture and the arts, the home, and even personal development through self-tracking and the quantified self. However, despite its ubiquitous use, a commonly accepted analytical definition of the term ‘big data’ has yet to emerge in the literature (Mittelstadt & Floridi 2016, p. 309). The most influential approach to date is the 3V Model, first proposed by data scientist Doug Laney (2001). According to Laney, dramatic increases in computer processing power, dramatic decreases in the cost of data storage, and the development and meteoric rise of the internet has ‘exploded data management challenges along three dimensions: volume, velocity, and variety.’ (Laney 2001, p. 1) It is the explosion along these three dimensions that, according to Laney, separates big data systems from traditional, or small, data systems.

The first V, ‘Volume’, rather simply refers to the sheer amount of available data. In the year 2000, it is estimated that there was around 800,000 petabytes of data stored worldwide, increasing to 1.2 zettabytes stored by 2010, and some estimates predicted that there would be over 35 zettabytes of data stored worldwide by 2020 (Kitchin 2014a, p. 70). To give an idea of scale, 1 petabyte is 1,024 terabytes, or over 1 quadrillion bytes. 1 petabyte is equivalent to taking more than 4,000 digital photographs every day over the course of an average lifespan, and it is estimated that the human brain can store around 2.5 petabytes of memory data (Fisher 2020). 1 zettabyte is $1{,}024^7$ bytes (in comparison a petabyte is $1{,}024^5$ bytes), or well over 1 sextillion bytes (1,180,591,620,717,411,303,424 bytes to be precise). To store one zettabyte of data requires more than one billion 1 terabyte hard drives and is roughly equivalent to over 250 billion DVDs. Of course, no one who is using big data is using over 35 zettabytes of data at once, nor is all that data stored in one centralised location. Kitchin (2014a, p. 71) suggests that a better way to understand Volume in this model is in regard to the rate and amount of produced data, as individuals, corporations, and governments increasingly use digital technologies and in turn generate more and more data.

‘Velocity’, in this model, refers to the difference in the rate of data generation and collection between big and small data (Kitchin 2014a, p. 76). Where small data, i.e. traditional forms of data collection and analysis, are performed sporadically and only capture snapshots of data at a certain time, big data allows for and relies on a constant stream of data collected in near real time.

As such, this ‘V’ is a measure of the increase in the rate at which data is generated, collected, and analysed.

‘Variety’ indicates that big data combines and links different kinds of data (Kitchin 2014a, p. 77). While both small and big data will utilise different kinds of data, ranging across structured, semi-structured, and unstructured data, small data is more likely to use one type of data for analysis. Big data on the other hand allows for the linking of data of different types and qualities, which in turn leads to a wider range of possible analysis.

Suggestions have been made to add further ‘V’s to the model, such as ‘Veracity’, referring to the uncertainty or messiness of the data that can be collected and used in big data in contrast to the precision needed for small data (Mittelstadt & Floridi 2016, p. 309) and ‘Value’, referring to the economic utility of big data for both businesses and governments (Chen et al. 2014, p. 173). However, for those who work with this model of big data, it is standardly described in terms of the three Vs of Volume, Velocity, and Variety.

While the V model is influential, it is not universally accepted as the best way to define big data. For some, the issue lies with the idea of Volume (boyd & Crawford 2012), as in many cases the data being referred to by the term big data are not (relatively speaking) all that “big”. For example, the data contained in all Twitter messages on a certain topic may be smaller in volume than the data contained in the US national census. As such, boyd[1] and Crawford suggest a definition of big data as the technological capacity to search, aggregate, and cross-reference large data sets to identify patterns, as well as a kind of mythology of higher intelligence and objectivity that surrounds the use of big data (boyd & Crawford 2012, p. 663). Mayer-Schönberger and Cukier (2013, p. 6) similarly argue that we need a more sociological definition of big data. As such they suggest that big data should be understood as a way of working with data on a huge scale, where we can extract new insights in ways that change society more broadly. Alongside the technological capacity to search large datasets for correlations, big data comes with three shifts in our mindsets:

> *The first is the ability to analyze vast amounts of data about a topic rather than be forced to settle for smaller sets. The second is a willingness to embrace data’s real-world messiness rather than privilege exactitude. The third is a growing respect for correlations rather than a continuing quest for elusive causality.* (Mayer-Schönberger & Cukier 2013, p. 19)

These shifts in mindset are, according to Mayer-Schönberger and Cukier, important parts of how we should understand big data, as they are both the results of the use of big data and important attitudes towards why we use it. Alongside this, they argue that ultimately big data is a predictive technology: ‘Predictions based on correlations lie at the heart of big data.’ (Mayer-Schönberger & Cukier 2013, p. 55). For Mayer-Schönberger and Cukier, the essential nature of big data is to make predictions, and as we use big data we develop a positive attitude towards using massive amounts of messy data to make predictions about human behaviour we have never been able to make before. Ultimately, while writers like boyd, Crawford, Mayer-Schönberger, and Cukier recognise that the technical aspects of big data must be included in its definition, they argue that we

[1] danah boyd (styled lowercase)

must look beyond just the technical aspects of big data and examine the mentalities that sit behind its use.

It is not necessary to choose between one of these various approaches, as they are not strictly in conflict with each other. What they all do is pick up on aspects of the umbrella term of big data, including the varying technologies that make up big data, the mindset or mentality that sit behind the use of big data, the inferential capabilities of big data, and the huge volume, variety, and velocity of the data used. All these aspects are key parts of big data, and recognising this helps us understand the many different technologies that fit under the umbrella of big data, and the many domains and contexts those technologies can be used in. As such, in this thesis, I will be using the term big data as a catch all term to refer broadly to all the technologies, capacities, and applications that make up big data.

What's the harm in a lot of data?

There are, of course, thousands of applications of big data, algorithmic analysis, and machine learning, and similarly thousands of possible ways for individuals to be harmed as a consequence of the use of big data. It is these harmful, or potentially harmful, applications of big data which are the focus of this thesis. More specifically, this thesis focuses on the ways in which the use of big data can both undermine individual autonomy and subject people to unfair discrimination. There are of course many other kinds of harm that individuals can face from the use of big data, but the prospects of unfair discrimination and limited autonomy are harms that are seeing increasing attention in the news media and in the literature, and are useful and important starting points for discussion. Importantly, these two harms are not mutually exclusive, and in fact overlap in some contexts, but I will briefly examine them here separately for clarity.

Firstly, big data can be used in a way that facilitates, or directly automates, decisions that unfairly discriminate against people. The operation of most algorithmic analysis and machine learning is to discriminate or sort between different variables and people, which in turn leads to the possibility of unfairly discriminating against those people. Indeed, we have growing reports of people who have faced discriminatory decisions that have been made based on algorithmic analysis or made by automated data-driven systems, and these reports come from highly varied areas of life.

We see instances of unfair discrimination in the context of employment. For example, O'Neill (2016, p. 105) describes the case of Kyle Behm, who faced discrimination based on disability (in his case bipolar disorder) in his search for employment. He was 'red lighted' by automated personality tests required as part of the application process. Despite his near perfect SAT scores and his attendance at the prestigious Vanderbilt University, his applications, even for minimum wage positions, were rejected every time he sat a personality assessment. These assessments were flagging him as not a good employee, and he could not progress past this automatic rejection. For those who do get jobs, as employers increasingly use data-driven tools to monitor and assess employees, the risk of unfair discrimination continues. Corporate wellness programs, where employers offer discounts for gym memberships, or weight loss and quit-smoking programs, have been married with big data to increase their effectiveness. For example, these systems can now predict with increasing accuracy an undisclosed pregnancy and even how far along the employee is in her pregnancy (Ajunwa et al. 2016, p. 475). While there is no evidence that anyone has been fired because a wellness program has guessed their pregnancy, they may then be treated in discriminatory ways by management as a result of the system figuring out this personal information.

There has also been growing attention on unfair discrimination from the use of big data by police forces, particularly in the US (Asaro 2019; Degeling & Berendt 2018; Griffard 2019). Police forces across the US are increasingly using predictive tools to help guide their decision making on who to intervene with early to prevent crime, who to investigate and arrest for crimes that have been committed, and where to patrol. However, there are concerns that these systems are racially biased, particularly those that predict the likelihood of criminal activity within a certain geographic area. This is largely because geographical location is a fairly consistent proxy for race in the US (O'Neil 2016, p. 87). As these algorithms operate, and direct police to particular areas, certain racial groups such as African Americans and Hispanic communities will be policed more, which can in turn establish a kind of feedback loop. Increased police presence means that more crime data is collected from these communities and fed into the system, which sends more police in response to the apparent rise in crime statistics.

Beyond the potential for unfair discrimination, the use of big data can also undermine individual autonomy and decision making, particularly around questions of self-determination. The Chinese social credit systems, where Chinese citizens and consumers receive score based on a wide range of past behaviour such as online purchases, who they know and interact with, and whether they are detected jaywalking, have been drawing attention recently in academic literature and in the media, and there are many who are concerned that it may be being used to limit the autonomy of Chinese citizens (Carney 2018; Chorzempa et al. 2018). For example, in one system those individuals who begin to lose points off their social credit score will face restrictions on which hotel rooms they can book, which extra-curricular activities their children can participate in, or even on whether they can get a mortgage (Raphael & Xi 2019). Additionally, over 11 million citizens have been blacklisted from buying flight tickets, and over 4 million have been blacklisted from buying high-speed train tickets (You 2018), effectively confining those people within their local area. The effect of this algorithmic ranking is that people have their options limited, and their opportunities for self-determination and development controlled by others, undermining their autonomy.

We can also see uses of big data which undermine autonomy more directly, where big data is used not to limit the options available to an individual but as the basis for directly depriving someone of their liberty. Criminal courts in the US have turned to algorithmic risk assessment tools to assist in sentencing and pre-trial bail hearings, and in some cases these algorithms are helping determine who gets bail or is kept in police custody before trial or the nature and length of a sentence. One example is that of Paul Zilly, who was convicted of theft in early 2013. During sentencing, an algorithmic risk assessment tool called COMPAS determined that he was at high risk of reoffending (Angwin et al. 2016). As such, the judge in this case sentenced him to two years in prison. While his sentence was reduced on appeal, the judge in the case stated that had he not seen the risk score he would have given a lighter sentence. In this way, the operation of big data can directly and unfairly limit or undermine the autonomy of individuals.

Of course, there are examples of uses of big data where we can see an overlap between unfair discrimination and the undermining of autonomy. One such case is the use of automated facial recognition technology, which can lead to unfair discrimination and the undermining of autonomy. The Chinese government has recently come under fire for using automated facial recognition as one of a suite of big data driven technologies used to surveil and control the Islamic Uyghur population of the Xinjiang region (Barbaro 2019). Upwards of one million ethnic Uyghur's have been relocated from their traditional homes into state run labour and re-education camps, and facial recognition has been a key tool for identifying people to be relocated into these camps, as well as ensuring those interned in the camps cannot escape. In this situation, we see both unfair discrimination against an ethnic group as well as the direct limitation of autonomy through labour camps and pervasive tracking.

Traditionally, individuals have been protected against these harms through privacy protections, but the use of big data analytics can result in individuals being harmed even where there are strong privacy protections in place. In many of these examples, including the cases of Kyle Behm, corporate wellness programs, the Chinese social credit systems, and Paul Zilly, individuals are being harmed by the use of big data despite existing privacy protections because privacy falls foul of the *inference problem*, where big data-based analytics can be used to infer information traditionally protected by privacy without technically breaching privacy rules.

This problem arises where an individual is subjected to a damaging adverse inference based on an algorithmically generated prediction. As our existing approaches to big data that rely on privacy are not effective, we must instead examine the ways in which big data can be used as a technology of privacy. Only then can we develop appropriate protections for individuals. This thesis will establish the foundations for such an approach.

Thesis Structure

Chapter 2 performs a ground clearing exercise and critiques arguments in the literature that reinforcing privacy rights is the best way of protecting people from harms that may result from the use of big data. Historically, new technologies such as photography and telephony have given rise to demands for new forms of privacy. I argue, however, that big data poses a unique challenge to the concept of privacy. By exploring three influential accounts of privacy, namely Tavani's account of Reasonable Access and Limited Control (RALC), Nissenbaum's account of Contextual Integrity, and Floridi's account of Informational Privacy, I will show that they all fall foul of what I call the *inference problem*. All these accounts of privacy share a common assumption that there is a form of information, i.e. personal information, that can be defined and classified in such a way that if we prevent the unauthorised movement of that information then we can protect the individual that information relates to from harm. However, big data allows for sensitive personal information to be inferred from data that we would not typically classify as sensitive, or even personal, information. Because we can now infer sensitive personal information, we can no longer make the assumption that sits at the heart of privacy, as personal information can be discovered and used without privacy being breached and the distinction between personal information and non-personal information is problematised. As such, we cannot solely rely on privacy as the foundation for our attempts to protect individuals from harm in the context of the use of big data, and we must look to other conceptual frameworks to address these gaps.

In Chapter 3, I argue that at the limits of a privacy focused approach to big data, we should examine the relationship between big data and power. However, I contend that there is no simple answer to the question of "what is power in the age of big data?", and that this is the wrong question to be asking. We should instead adopt a pluralistic attitude towards power which allows us to see how different kinds of power operate across different contexts. First, I examine several writers who each propose an account of big data power. Across these writers, there is a common attitude that the development of big data leads to a kind of revolutionary or epochal shift in the nature of power. Against this view, I argue that just as we should understand big data as a kind of umbrella term, we should also understand power as a kind of umbrella term that refers to a wide and diverse range of phenomena. The concept of power resists a unified and comprehensive definition, and only by recognising the pluralistic nature of power can we properly understand the ways in which different kinds of power use big data in different ways. To demonstrate the varying ways we can understand power, I will present a rough taxonomy of seminal accounts of power, categorised into causal, procedural, and productive accounts of power. Following this taxonomy, I sketch out a series of focused questions which help to identify different modes of power, in order to move towards a more pluralistic understanding of power. So, rather than asking general questions such as "what is power in the age of big data?", we instead examine a more specific context in which big data is being used as a technology of power, and ask "what is the intended outcome of power?", "who is exercising power?". "Who is power exercised on?", and "how does this power function?". By asking these questions, we can identify key contextual features of the mode of power we are analysing, which will in turn help us identify the relevant conceptual features of different theoretical accounts of power present in that context. By using this approach, we can avoid oversimplifying and missing key elements of the operation of power in a context.

In Chapter 4, I will use four examples to demonstrate the value of adopting a pluralistic attitude towards power, as it allows us to understand the operation of power within a given context in a nuanced way. Firstly, I will look at the operation of the Chinese social credit system, and see how the features of that context, namely the goal, agent, subject, and means of the mode of power align with the key features of Foucault's account of power. Then, we will use the same approach to examine the operation of power in the context of Amazon's use of big data to manage employees. In this example, we can see key features of both Foucault's and Parson's account of power, which overlap as a kind of hybrid form of power. The third example is the use of automated facial recognition technologies by law enforcement agencies, in which we can see many of the key conceptual features of Dahl's account of power. Finally, in this chapter we will look at the use of big data by governments and health agencies to track and contain the spread of COVID-19. Here, we can see features from Parson's, Foucault's, and Hobbes' accounts of power, overlapping with each other and working in parallel in this context.

In Chapter 5, I will expand on my argument that big data has not necessarily led to the development of a whole new kind of power, but instead can be and is used by "existing" kinds of power. Others who consider the relationship between big data and power argue that the development of big data requires us to develop new theoretical understandings of "big data power", or that the development of big data has in some way made older kinds of power redundant. Here, I show that this is not necessarily the case, as we can see important historical continuities in the operation of power both before and after the development of big data. To show these continuities, I will compare the operation of power between the Chinese social credit system and the Medieval Catholic Church, between Amazon's workplace management techniques and the Ancient Roman *cursus publicus*, between how police use automated facial recognition and early fingerprinting technology, and between modern pandemic tracking and 17th century plague management. From the similarities in these contexts, we can see the impact of big data as making power more efficient, increasing the range of power, and increasing the effectiveness of power, but not leading to a whole new kind of power.

Chapter 6 examines an impact on power that is unique to big data. While it has inherently not led to the development of a new kind of power, big data is still a revolutionary technology with unique inferential capabilities. Big data allows us to uncover previously invisible correlations and detect patterns in sets of data. These correlations and patterns allow us to draw inferences about both the past and future and make ever more accurate predictions about the world around us and human behaviour. These novel inferential capabilities lead to a crucial shift in the operation of power; namely the subjects on which power directly acts are, increasingly, not people but data doubles. I here define data doubles as fragmentary digital representations of a person that both contains and can be used to make predictions about that person. This shift underpins a broader ethical problem, namely the undermining of accountability. As data doubles are targeted as the subject of power, it becomes harder to monitor the operation of power, to challenge exercises of power and impose sanctions in response to abuses of power, and it becomes too difficult to justify exercises of power.

Finally, in Chapter 7, I will examine four more contexts using a pluralistic approach to power to show how exercises of power shift towards targeting the data double, and what impacts this has on our ability to ensure that power is exercised in accountable ways. The first context in this chapter is the use of algorithmic risk assessment tools in the American court system. In this example we see the key features of Weber's and Foucault's accounts of power, and the shift to the data double changes the importance of knowledge to the operation of power. This makes it harder to ensure that power in this context is exercised accountably. In the second example, I look at the use of predictive policing technologies, and focus on how Dahls' account of policing power is altered by the use of big data as the legitimacy of police power is undermined through an inability to keep power accountable. The third context is the use of targeted advertisements in election campaigns, which clearly displays the key features of Machiavelli's account of power. While it is already hard to ensure that exercises of Machiavellian power are accountable, the shift to the data double makes it even more difficult to do so as the exercise of power becomes invisible. Finally, we will look at the operation of power in the smart city, where we can see the features of Foucault’s, Hobbes’, and Lukes’ accounts of power overlapping each other. The use of big data here makes power less accountable as it amplifies the strength and subtlety of power in this context.

Chapter 2

Privacy

The academic literature surrounding the ethics of big data is largely focused on the concept of privacy. This focus is primarily on discussions of how the development of big data presents new problems for current privacy protections, and how we can go about updating those practical protections as well as our conceptual understanding of privacy. A meta-analysis of the literature in 2016 indicated that those papers written about the ethics of big data covered five major themes, the second most common of which was privacy (Mittelstadt & Floridi 2016, p. 309). Those who write about privacy and big data are often concerned about how big data can lead to breaches of privacy (Mittelstadt & Floridi 2016, p. 316), such as through:

- Invasive data collection and analysis, where combined data sets including geolocation data and internet-based sources can be used to collect detailed and often sensitive personal information;
- Increased scope of data collection, where limitations of human memory and perception are no longer barriers to the collection of information from people; and
- The longevity of collected data, where information that is collected is far less likely to be forgotten and can be used indefinitely (this is more a concern about future breaches of privacy).

Data brokers, Silicon Valley technologists, and other figures who are invested in the rise of the data industry of course have an interest in calling for the end of privacy, typified by the comments of Facebook founder Mark Zuckerberg, who suggested that privacy is no longer a social norm, and the rise of social media is both a sign of this shift and a contributing factor to the declining relevance of privacy (Johnson 2010). But in the academic literature, we see a strong trend in the opposite direction. Most writers argue that privacy is still a relevant and important social norm, but that it needs to be reimagined or updated in some way in order to meet the challenges posed by big data. Writers who make arguments along these lines include Nissenbaum, whose account of privacy as contextual integrity has become a dominant account (Mittelstadt & Floridi 2016, p. 316), and writers including Mittlestadt, Floridi, Taylor, and van der Sloot who have developed accounts of group privacy and inferential privacy (Taylor, Floridi & van der Sloot 2016; Floridi 2016; Mittelstadt 2017).

While we should resist the view that privacy is now socially irrelevant, in the context of big data our current understandings of the concept of privacy have become outdated. Privacy, as a set of legal rights and protections, is no longer an adequate tool when it comes to the new kinds of unfair discrimination and undermining of autonomy that arise from the use of big data. Fundamentally, the concept of privacy is ill-suited for dealing with big data. This is because privacy rests on a basic assumption around a form of information called “personal information”, or sensitive information that is about or related to a person and can be used to positively identify them and/or convey or inform an opinion about a person. The assumption is that there is a form of information called personal information that can be defined and classified in such a way that if we prevent the unauthorised movement of that information then we can protect a person from harm from the use or misuse of that information. In other words, privacy only functions if we can identify sensitive personal information and can prevent unauthorised access to that information or movement of that information between others. It is this core assumption that means that privacy cannot solely cope with the challenges posed by big data, because large scale data analysis leads to what I will refer to as the *inference problem*.

The inference problem is concerned with the way in which big data-based analytics, particularly AI and machine learning, can be used to infer information that is traditionally protected by privacy without "breaching" privacy in traditional ways. This problem arises because big data allows for personal information to be inferred through the algorithmic analysis of other, often apparently unrelated, items of information. This leads to a break down in the adequacy of privacy for two reasons. Firstly, the use of big data means that the practical mechanisms of privacy can be avoided "private" personal information can be discovered and used in decision-making processes in ways that do not breach privacy protections. Because we can infer personal information by using big data, we can use unprotected information to discover what would normally be protected by privacy. Secondly, because of this ability to infer personal information from information that seems otherwise unrelated, in the context of big data we can no longer differentiate between personal and non-personal information. This destabilises the basic assumption behind our current understandings of privacy, and as such big data does not just avoid privacy protections in a practical sense, but also undermines the adequacy of theoretical understandings of privacy.

To outline this argument, firstly I will examine three influential contemporary accounts of privacy, drawn from Moor and Tavani, Nissenbaum, and Floridi. These three accounts of privacy are constructed in very different ways, yet they all rest on a central assumption whereby personal information can be protected in order to protect individuals from harm. Following this, I will explore in more detail how this central assumption makes privacy ill-suited for dealing with the challenges posed by big data, including in the face of new, big data-focused, accounts of privacy such as group and inferential privacy.

Conceptions of Privacy

While we may be quick to complain when our privacy is invaded, we immediately run into difficulties in explaining exactly what we mean by privacy (Tavani 2008b, p. 131). As some authors have argued, there is an instinctive or innate desire in most animals for seeking 'periods of individual seclusion or small-group intimacy' (Westin 1984, p. 56). Seeking time alone and away from other members of the group or species provides benefits to both the larger group, by allowing for careful selection of mates, ensuring safe spaces for the young to grow and learn, and avoiding overuse of local resources, and to the individual, by increasing chances of detecting danger and courting, and potentially even reducing the risk of illness or death as a result of stress induced endocrine failure (Westin 1984, p. 58). It seems likely that this instinctual need for 'periods of individual seclusion' has gone on to inform a view of privacy focused on protection against or prevention of physical intrusion by others.

Early notions of privacy are largely concerned with the desire for seclusion or small-group intimacy. Ancient legal codes such as The Code of Hammurabi, one of the world's oldest deciphered writings from Babylon around 1750 BCE, protects the private home from intrusions by others, and ancient Roman laws provided for the same protection (Solove 2011, p. 4). We can also see the development of the protection of privacy in terms of physical access to the home in the evolution of the early torts of trespass and nuisance in 14th century England (Vincent 2016, p. 8). At the time, members of a household would often live in tight quarters as buildings rarely had internal walls. As such, the developing torts of trespass and nuisance fiercely protected the home from unwanted external intruders or access. In many ways, 'an open or closed door was both a symbol and a reality' (Vincent 2016, p. 13), and while citizens of the Babylonian or Roman empires or of medieval England would not say that they had a right to privacy, they certainly believed they had a general right to not be interfered with, at least in regards to the four walls of their homes.

However, as new communication technologies developed, these accepted norms of privacy were challenged. Modern conceptions of privacy still in use today largely developed in the late 19th century in response to new technological developments in publishing (Igo 2018). The development of 'instantaneous' photography, telegraphy, telephony, and sound recording, which in turn led to dramatic developments in mass media and gossip magazines, gave rise to urgent questions about what privacy was. Until that time, it was largely linked to physical proximity, so it was only possible to breach privacy by intruding physically on a person, whether that be by entering their home or directly watching them (Igo 2018, pp. 17-18). Conceptions of privacy had to change, and American lawyers Samuel Warren and Louis Brandeis published an article in 1890 arguing that the courts should understand privacy as a right of the individual to be free of interference and intrusion; in other words that privacy is best understood as the "right to be let alone" (Warren & Brandeis 1984).

Warren and Brandeis briefly traced the development over time of what it means for an individual to have full protection of their person, starting from early legal codes that protected the right to life and rights against physical intrusion, to more recent legal codes that began to protect mental states through laws against assault and nuisance as well as the protection of intellectual property through copyright. However, they called for the law to continue this project and update its conceptions of privacy. In the late 19th century, the rapid spread of 'instantaneous photographs' fuelled a growing news industry focused on tabloid news and gossip columns (Warren & Brandeis 1984, p. 76). These new technologies and social conditions, according to Warren and Brandeis, posed a significant problem to existing conceptions of privacy, and to protect individuals from the harms they might suffer should private thoughts and incriminating photographs be published widely they argued that the law should protect privacy as the right to be let alone. The right to privacy, which had in the past been seen as a subsidiary right as part of the right to property ownership, must now become a right in and of itself, a right to one's personality, i.e. the right to present yourself as you see fit and protect yourself from misrepresentation by others (Warren & Brandeis 1984, p. 83).

Warren and Brandeis' work on privacy has remained influential but privacy law has struggled to keep up with new information and communication technologies. The massive increases in computer processing power, decreases in the costs of data storage, and the rapid spread of interconnected digital devices that make up the internet of things that have enabled the development of big data, lead to tremendous challenges for privacy protections. One response is to attempt to redesign privacy, to update it to fit the challenges of the digital age just as Warren and Brandeis and others have reframed privacy to cope with past technological and social developments.

This instinct to turn to privacy and information ethics more generally is an understandable one. After all, big data is, broadly speaking, an information communication technology, and the history of privacy is a history of reactions to the development of new information communication technologies. The development of cameras is a prime example of such a technology, where existing understandings of privacy had to be updated in response to new technological capabilities. But we can no longer rely on privacy to cope with big data. This is not to say that privacy is no longer a social norm, as Mark Zuckerberg infamously remarked (Johnson 2010). We still need and can rely on privacy rights in a wide range of contexts, such as in a doctor's office. But we cannot solely rely on privacy to meet the challenges of big data, because big data undermines the core assumption of privacy. To show this, I will now explore three influential contemporary accounts of privacy, namely Moor and Tavani's account of Restricted Access and Limited Control, Nissenbaum's account of Contextual Integrity, and Floridi's approach to Informational Privacy, in order to show how big data problematises the protections that privacy offers.

Restricted Access and Limited Control (RALC)

Moor and Tavani propose an account of privacy they refer to as the Restricted Access and Limited Control (RALC) account of privacy (Moor 1997; Tavani 2007; Tavani & Moor 2001). In this account, privacy is best understood as a series of overlapping zones of privacy, which individuals then have the right to exert control over, and this control is largely operated to restrict those who may gain access to those zones. In short, this account of privacy is concerned with how disastrous it would be for people to lose control over who can access their personal information, and thus looks to ground the right to privacy as a right to self-determination and autonomy. This approach to privacy is largely informed by Rachels' (1975) arguments about the value of privacy. For Rachels, the value of privacy comes from its necessity in maintaining social relationships, as it is an essential tool for ensuring control over access to yourself or information about yourself. Without the ability and right to control access to personal information, it is impossible to maintain different social relationships and keep them distinct from each other. As an example, there are currently many countries where it is illegal to be openly homosexual, including several countries such as Afghanistan, Iran, and the United Arab Emirates who prescribe the death penalty for same-sex sexual activity between men. For members of the LGBTQ+ community in those cultures, the right and ability to actively control who has access to their personal information is of vital importance for their safety, and in some cases for their lives.

Under RALC, an individual has privacy 'in a situation with regard to others [if] in that situation the individual . . . is protected from intrusion, interference, and information access by others' (Moor 1997, p. 30). Moor uses the word "situation" to cover not just physical locations but also relationships, activities, and any other area of life. So, under RALC, privacy is best understood as existing in overlapping "zones" (Tavani & Moor 2001, p. 7). Essentially, these zones of privacy can be carved out of everyday situations such that they are embedded in and overlap in complex ways. An example that Moor and Tavani use is of a woman having a private phone conversation while sitting in a public building and holding a purse. While this woman can be viewed easily by those around her, her phone conversation is private except for any individual who may be sitting nearby who can hear one side of the conversation, and the contents of the purse are completely private from those around her. Across these areas or zones there are different expectations and rules of privacy.

Importantly, RALC differentiates between normative and natural privacy (Moor 1997, p. 30). A normatively private situation is one that is private because it is protected by some ethical, legal, or conventional norm, whereas a naturally private situation is one that is private because of some natural shield such as a physical barrier. For example, a conversation between a doctor and a patient is normatively private, as it is protected by ethical, legal, and conventional norms, but it is also often a naturally private situation, as onlookers are rarely encouraged in a doctor's office. Importantly, natural privacy can be lost but not violated, while normative privacy can be both lost and violated. If someone were to be having a conversation with a friend in a secluded area of a park, they would have natural privacy that would be lost the moment someone else walked nearby, but they would not have had their privacy violated. However, if that same stranger had walked in on someone's doctor's appointment, there would be a loss of natural privacy and a breach of normative privacy. So, in short, RALC holds that privacy exists across different and overlapping zones of normative and natural privacy.

These zones require management, and this is the second element of the RALC account, and where control becomes important. For the practical management of zones of privacy, individuals need to have some reasonable control over both that zone and the flow of information in that zone. This control is not absolute, and as such Moor constructs privacy in terms of access rather than control. Control here should be understood as a combination of choice, consent, and correction (Tavani 2007, p. 12). An individual has the right and ability to choose which situations or zones of privacy they enter into, as well as their right and ability to consent to others accessing those same situations or zones, and of course the right and ability to correct any information about themselves. In this way, the concept of privacy is designed to protect the autonomy of individuals, in terms of self-determination and their ability to develop their own unique identity. In doing so, it can also protect individuals from discrimination based on these developing identities, such as LGBTQ+ communities in countries that outlaw such practices.

To highlight the operation of RALC, Tavani looks at data mining. As RALC is focused on different situations or zones of privacy, Tavani argues that by using this framework we can assess data mining as a situation to determine whether there should be a protection of a normative kind of privacy (Tavani 2007, p. 15). In this case, the answer is that there is a normative sense of privacy here, based on Moor's Publicity Principle, which holds that the rules and conditions of private situations should be clear and known by those affected by those rules and conditions (Tavani 2007,

p. 16). In this situation, as personal information is mined, where there is an instance of data mining that is performed covertly or in a way that is opaque to those affected by it, we can say there has been a breach of normative privacy. Conversely, where there is an example of data mining that is performed openly and transparently, there is not a breach of normative privacy, as the rules and conditions are clear and arguably known.

Contextual Integrity

Nissenbaum's (2004, 2010, 2011, 2018) Contextual Integrity (CI) approach has become an influential approach in the literature (Falgoust 2016; Hull et al. 2010; Mai 2016; Matzner 2014; Mittelstadt & Floridi 2016). There are two main problems that Nissenbaum is looking to answer with this approach to privacy. The first problem is that the development of big data has led to a number of overlapping technical capabilities, including tracking, monitoring, aggregating, analysing, disseminating, and publishing information, and these overlapping capabilities make it difficult to assess the ethical impacts of big data on privacy using traditional accounts of privacy (Nissenbaum 2010, p. 11). To solve this problem, Nissenbaum has developed the CI approach to avoid relying on theoretical definitions of privacy, and instead to operate as a kind of decisional heuristic, such that we can pick out the details of a given context and identify the norms of privacy at play easier than appealing to broader principles. The second problem is that as new technologies are developed, we do not know how they will impact on values surrounding privacy. This approach then looks to provide a way for us to predict how people will use and respond to a new technology by examining the norms that begin to develop around the use of that technology (Nissenbaum 2010, p. 2).

Ultimately, in CI, privacy is the right to the appropriate flow of personal information (Nissenbaum 2010, p. 127). Whereas traditional accounts of privacy, and contemporary accounts more closely inspired by them like RALC, describe privacy as a right to secrecy or a right to the control of personal information, the key word in this right is "appropriate". Within a given context, there are expectations and norms surrounding the movement of personal information, for example there is a general expectation that personal information provided by a patient to a doctor is kept private from the general public but may be transmitted to a nurse or health specialist when necessary. The right to privacy then is the right to expect that personal information only moves according to these general expectations and norms. This is a more practical approach to privacy, according to Nissenbaum, than traditional accounts. Where traditional accounts of privacy look to define privacy at a theoretical level then build protections up around that, this approach functions as a kind of decisional heuristic, where individual contexts can be examined to pick up on how privacy functions in the real world, as well as how new technologies interact with existing expectations and ideas of privacy (Nissenbaum 2010, p. 148).

Nissenbaum's use of the word context here is similar to that of Moor and Tavani's use of situations or zones, but Nissenbaum provides a more detailed description of what to look for in a given context, namely roles, activities, norms, and values (Nissenbaum 2010, p. 132). Roles are the different parts that actors play in those contexts, such as teacher, voter, patient, client, parent, friend, or employer, amongst many others. Activities are, straightforwardly, the actions and practices an actor can perform in that role. These activities can be strictly controlled and structured, such as the act of voting or teaching, or loosely controlled and unstructured, such as browsing in a store or providing comfort to a friend. Norms are the rules that determine the relevant actors in a context, as well as the activities those actors can perform. These norms can also be structured or unstructured, such as laws and codified regulations or etiquette and community pressure. Finally, there are also values, or the reasons why the norms, activities, and roles exist. For example, in a healthcare setting, the value of helping the sick and promoting health are why we have actors like doctors and nurses, activities like surgery and writing prescriptions, and norms such as drug regulations and pressure to seek help when sick.

Within a context, there are of course a large, if not infinite, number of potential norms that could apply, but the Nissenbaum is primarily concerned with informational norms, i.e. norms about the flow of information. When looking at contexts generally, informational norms govern three main things (Nissenbaum 2010, p. 140). The first are the actors. Informational norms have places for three types of actors; the sender of information, the receiver of information, and the information subject (who may or may not be the person sending or receiving the information). These roles can overlap with others, so in a context containing a lawyer and a client, they can at different times be the sender and receiver of information as well as the information subject. Informational norms also govern the types or nature of information that can be sent, such as medical history, postal address, appearance, criminal record, etc. Finally, informational norms also govern transmission principles, or the constraints on the flow of information. Such constraints could include things like confidentiality (only certain actors can receive it), compulsion (an actor must send it even if they don’t want to), and the method of transmission (in person, over the phone, via letter, etc).

So, when investigating whether there has been a breach of privacy, the question to ask is ‘Does the practice in question violate context-relative informational norms?’ (Nissenbaum 2010, p. 148). To answer this, we then ask four sub-questions:

1. What exactly is the context – i.e. is it obvious or does it overlap with others; is it novel or traditional?
2. Who are the actors in this context?
3. What types of information are being transmitted?
4. What are the transmission principles in this context?

If the practice being investigated makes a change to either the actors involved, the type of information being transmitted, or the transmission principles, then there is a prima facie violation of informational norms and therefore a violation of privacy. So, for example, in an obvious and traditional context such as a doctor’s office, should a doctor tell her husband the medical history of a patient, there is a change in the actors involved and the transmission principles (namely confidentiality) and therefore a breach of privacy.

Floridi’s Informational Privacy (IP)

Floridi’s account of Informational Privacy (IP) is aimed at addressing what Floridi feels is a lack of nuance in the literature on the ethics of big data and information technologies more generally (Floridi 2005). Floridi is responding to what he refers to as the ‘2P2Q’ hypothesis, namely that digital information communication technologies (ICTs) are exacerbating existing problems for privacy because of the dramatic increases in data *Processing* capacities and speed (or *Pace*), as well as the *Quantity* and *Quality* of the data that can be collected and managed (Floridi 2005, p. 186). This 2P2Q hypothesis is a pre-cursor to popular definitions of big data technologies, particularly the 3V (or 5V) model. However, he argues that this hypothesis does not capture the whole story, and that these new ICTs, which working with his definitions here would include big data, can both lead to potential increases in privacy in some respects. So, while the data mining capabilities of big data may be concerning in that they allow for invasions of an individual’s privacy, big data can also be used in ways that reinforce privacy, such as by using biometrics for security purposes or using algorithmic tools to generate secure passwords. The problem then that Floridi looks to tackle with his account of IP is addressing how big data, and other ICTs, can be used in ways that can either preserve or undermine privacy.

To answer this problem, Floridi positions IP as a part of his somewhat controversial (Capurro 2008; Doyle 2010; Ess 2008; Leeuwen 2014; Tavani 2008a), ontological project of assessing the world as being fundamentally informational in nature. The full details of this project are beyond the scope of this thesis, and will not be explored in full, but it is important to recognise the background it gives to Floridi’s account of IP. Briefly, Floridi argues that in order to address a specific problem or answer a specific question, it is necessary to understand the level of abstraction at which that problem or question exists, and then utilise that same theoretical framework in order to arrive at coherent solutions or answers (Floridi 2008a, p 190). Therefore, it is necessary to adopt the appropriate level of abstraction, as this choice determines the relevant questions to ask, the answers being sought, and the affordances that can be made. So, when examining questions surrounding informational privacy[2] it is necessary to adopt an informational level of abstraction, whereby the world and its inhabitants should be understood informationally.

Then, when adopting an informational level of abstraction, Floridi argues that we should see ourselves and everything in the world around us as informational entities, and organisms with agency, such as humans, as special kinds of entities called informational organisms or *inforgs* (Floridi 2014a). While a full exploration of informational entities and organisms is beyond the scope of this thesis, what is relevant here is that an informational entity such as a chess piece is a collection of self-contained packages of data structures that constitute the nature of the object, such as its position on the board and its colour, and functions or procedures activated by stimuli that govern the object’s reactions, such as where it can move (Floridi 2002, p. 288-9). An *inforg* then is a kind of informational entity that can process information logically and autonomously (Floridi 2014a, p. 94), such as a human, who can then interact with other informational entities like a chess piece.

The world itself can also be understood informationally, as an *infosphere* (Floridi 1999, 2002, 2005), an analogue of the biosphere or ecosphere, which serve as key concepts in the work of

[2] Floridi’s account of IP is an account of informational privacy, one of four kinds of privacy that Floridi identifies, including physical privacy, decisional privacy, and mental privacy.

many environmental ethicists (Tavani 2008a, p. 157). The infosphere is essentially made up of the informational entities that inhabit it, as well as the total sum of all their interactions. It is in the infosphere that Floridi's account of IP functions. In short, IP is the inverse function of the informational friction of the infosphere around us, i.e. how easily information moves between inforgs (Floridi 2005, p. 186). This friction arises from both the features of the environment and the capabilities of the various inforgs that inhabit that environment. For example, as humans cannot see through a solid brick wall but may still hear loud noises from behind it, the presence of a brick wall obscuring line of sight will afford a certain amount of privacy within the infosphere. However, should that wall suddenly become transparent or should a CCTV camera be mounted on the wall, the privacy afforded by the wall would vanish. For Floridi then, violations of privacy are associated with reductions in information friction.

As Floridi characterises it, the right to privacy is:

> *… the right of individuals (be these single persons, groups, or institutions) to control the life cycle (especially the generation, access, recording, and usage) of their information and determine when, how, and to what extent their information is processed by others.* (Floridi 2014a, p. 114)

To exercise this right then is to control the friction of the infosphere. In IP, there is a distinguishing between both natural and normative privacy. Natural privacy comes from "naturally" occurring sources of friction such as solid walls, and while it can be lost it cannot be violated. Normative privacy comes from "non-naturally" occurring sources of friction, such as laws or social norms that restrict the movement of information. The right to privacy is the right to enforce those non-natural sources of friction, and to breach those rights is to act in a way that reduces the friction in the infosphere in a way that the right-holding individual(s) did not authorise or consent to.

Interestingly, if we accept Floridi's ontological account, a breach of privacy is less like trespass or theft, and more akin to kidnapping or false imprisonment (Floridi 2006, p. 112). If we accept that we can be understood as *inforgs*, entities constituted by various packages of personal information, a breach of privacy whereby that information is 'taken' by someone else is not a theft of property, but a kidnapping, as it is a taking of the information that makes us up. Where traditional accounts of privacy would see a breach of privacy as the theft of property, somewhat analogous to stealing a car, Floridi suggests that a breach of privacy is more analogous to kidnapping, as the "breacher" of privacy gains control over another person's identity. However, it is not necessary to accept Floridi's broader ontology in order to accept his general ideas around the nature of privacy. In this case, Floridi's approach to privacy is a method by which we can control the rate at which information moves between people. Naturally, privacy can be found where information cannot easily move between people, but we also have normative rights to privacy which allow us to insist on non-natural barriers to the flow of information.

Personal Information

These three accounts of privacy all share a common assumption at their core. This assumption is that a form of information, personal information, is defined and classified in such a way that if we prevent the unauthorised movement of that information then we can protect the individual that information relates to from certain kinds of harm. There are two parts of this core assumption, the first being that we can identify a certain kind or kinds of information, and that the prevention of its movement is what protects individuals from harm. The first part of this assumption is that a requirement for privacy to function is to clearly identify the information that is protected by a right of privacy. Personal information does not have a clear definition, but it is generally used to refer to information that is about or related to a person. This includes information that can be used to positively identify a person, information about a person's actions or activities, and sensitive information that may also convey or inform an opinion about a person such as information about a person's race, sexual orientation, political or religious beliefs, or health, amongst other kinds of information about a person.

In RALC, we identify the relevant personal information to be protected based on the relevant situation or zone of privacy. So, if we are looking at a zone of privacy around a consultation with a doctor, the relevant personal information would be any information about the health of the patient, as well as potentially sensitive identifying information such as name or home address. This zone is then kept private only so far as the relevant identified information is concerned. In CI, the relevant personal information is picked out by the third part of the decisional heuristic, namely the question "What types of information are being transmitted?" To establish the relevant contextual norms, it is first necessary under this approach to identify the information that is being transmitted. Without that knowledge, we cannot use CI to determine whether the concept of privacy applies, let alone whether it has been breached. If, as Floridi suggests that privacy is the right of individuals or groups 'to control the life cycle … of their information and determine when, how, and to what extent their information is processed by others.' (Floridi 2014a, p. 114), then it is necessary that we can identify what information belongs to a person as "their information". In this approach, the relevant information will be any information that is constitutive of a person's identity as an inforg, namely those pieces of information that constitute the nature of the inforg as well as the various actions and responses they have to different stimuli.

In the second part of this core assumption, once we have identified the relevant pieces of information, if we can prevent the unauthorised movement of this information then we can protect the individual from various harms. It is this movement that makes up the core practical part of privacy. The personal information protected by privacy must be obtained in some way, and to protect individuals from harm the right of privacy prescribes ways in which that information can be obtained or "moved". So, in RALC, once the relevant personal information is identified, the person it relates to has the right to limit access to that zone and control the movement of that information between individuals within that zone or situation. In CI, the main purpose of the decisional heuristic is to set out the norms that regulate the movement of information between individuals, so when the elements of the context have been set out (including the information being protected), we can determine how that information should move between people in order to protect individuals from harm. Finally, in IP, privacy is a function of the friction present in the infosphere. As such, to increase privacy, it is necessary to make it harder for information to move between inforgs, while a decrease in privacy is a result of easier movement of information.

The Inference Problem

All three of the approaches above depend on an assumption that privacy can be protected if we can effectively control the unauthorised movement of personal information. I will argue that it is no longer possible to make this assumption regarding the use of big data because of what I refer to as the *inference problem*. The inference problem is the way in which big data-based analytics, particularly AI and machine learning, can be used to infer information that is traditionally protected by privacy without breaking existing privacy laws. The inference problem arises from the way in which big data analytics can infer personal information without needing to access that information. One of the primary functions of big data is to perform correlation-based analysis, to detect patterns in large swathes of data that would otherwise be difficult if not impossible to detect. This analysis can be used to infer information about people more effectively than ever before, and it is this ability to infer information that shows us the limitations of protective frameworks based on privacy alone. There are two significant implications of the inference problem: the identification of individuals, and the problematising of the definition of personal information.

The first implication of the inference problem is that big data can be used to make statistical inferences about personal information. Existing privacy laws do not protect against the discovery of sensitive personal information by analytical inference from unprotected data. A breach of privacy typically occurs when personal information moves in an unauthorised way from some source. Privacy protections rely on this movement, whether that be as a result of an individual losing control over their own personal information, a breach of some contextual norm leading to an inappropriate flow of personal information, or because some action has decreased the friction in the infosphere allowing information to move more freely without consent or authorisation. However, where big data is used to infer personal information, we cannot say that it moves in the same way. Those pieces of personal information that would normally be protected by privacy can be inferred from other, readily available kinds of information. This may be because those pieces of information are not classified as private information or are collected with consent and thus their use is authorised (for example, in a *Terms of Service* agreement). In this process, privacy protections over personal information are essentially bypassed because they can be inferred.

For example, in what is now an infamous case of the use of big data in targeted advertising, the American retailer Target used big data to predict the pregnancies of customers in order to send out precisely timed and targeted advertisements (Mayer-Schönberger & Cukier 2013, p. 58). The company analysed the purchases of women who had signed up to for Target's baby gift-registry and developed a pregnancy prediction score which it would assign to female shoppers. In one case, this advertising material was sent out to a teenager who had not yet told her family she was pregnant, prompting outrage over alleged violations of privacy. In a similar vein, researchers at Cambridge University, UK, developed an algorithm that could predict a person's race 95% of the time, gender 93% of the time, whether a man was heterosexual or homosexual 88% of the time, and whether someone was a registered Democrat or Republican 85% of the time (Kosinski et al., p. 2). These predictions could be made only through algorithmic analysis of the pages that person had “liked” on Facebook, even where those pages did not obviously convey or relate to the inferred personal information. In these and similar situations, sensitive personal information was inferred from information that was collected with consent, such as a history of purchases or page likes, without breaching privacy protections.

The same is true in terms of identifying an individual from a database. A standard technique that is used to provide privacy for an individual whose data ends up in a database is to anonymise or de-identify the information stored in the database (Mittelstadt & Floridi 2016; Ohm 2009). To anonymise a database, firstly personal identifiers like names and addresses are deleted and secondly context specific identifiers like student ID numbers, bank account numbers, or the names of next of kin are removed from the database (Ohm 2009, p. 1703). However, even where these personal identifiers have been removed, it is still possible to positively identify an individual by using the information still left in the database, and often with only a very small number of data points (Matzner 2014, p. 98). It was even shown that an individual could be identified in an anonymised database from the streaming service Netflix using only the ratings that person gave to six movies (Ohm 2009, p. 1721). So long as the data contained “pockets of uniqueness”, data combinations that were unique to a given individual, they could be used to create a sort of data fingerprint, and then used to positively identify an individual. Despite attempts to protect privacy, big data allows for pieces of personal information or the identity of a person to be inferred in ways that circumvent those protections entirely.

Within the literature, there are writers who advocate adopting a conception of group privacy, and while these accounts may at face value appear to offer a solution to this first part of the inference problem, they still run into the same issue. For example, Mittelstadt (2017) argues that an account of group privacy, where individuals have a right of privacy as a right of inviolate personality based on their identity as a member of a group, while Floridi (2016) proposes an account of group privacy whereby certain groups, such as families, have a right to the protection of group information as private from outsiders. In either case, the argument can be put that this group privacy can protect individuals from the inference problem by offering rights for individuals against identification as a member of a group. But these protections are largely an extension of traditional privacy protections, and run into the same problems, whereby individuals can be easily identified through algorithmically derived inferences. While group privacy may be appropriate in some contexts, it does not fully overcome the inference problem.

The second implication of the inference problem is the problematising of the definition of personal information. In short, the operation of big data problematises the definition of personal information as a category of information. Researchers at the University of Toronto have developed a mobile phone app called Anura, which infers the age of the user, as well as predicting their life span and the chance of developing (or currently having) a number of diseases such as cardiovascular disease, high blood pressure, heart attack, and stroke, all from a single photograph or selfie (Dormehl 2019). The app works through a combination of facial recognition and transdermal optical imaging, where photographs are analysed algorithmically to detect how infrared light bounces off the haemoglobin protein in our skin. Another group of researchers at New York University have developed an AI that can detect PTSD in a person, so long as they are a male, and in the military, only through their voice (Coleman 2019). The AI has been trained on thousands of speech samples and has learned to detect patterns such as tension in throat muscles and whether the tongue touches the lips that indicate the likelihood that someone has PTSD. Finally, a personality test developed by the workforce management company Kronos and used to filter out job applicants appears to infer mental health conditions in those who take the test. One man was rejected from dozens of jobs that used this test, which appeared to be excluding him from the selection process by inferring his bipolar disorder (O'Neil 2016, p. 106).

In these and similar cases, it is either not clear that privacy is the relevant conceptual framework, or that framework cannot alone offer protections against harm. This is because big data allows for the use of information not typically considered as "personal" in inferring "personal information". While we may still be able to point to certain information and clearly say "this is personal information", big data means it becomes increasingly difficult to determine whether other pieces of information are *not* personal information, or at least do not allow us to discover personal information. Consider the use of an AI to detect PTSD. A medical diagnosis of PTSD is a straightforward example of sensitive personal information, and like all other medical diagnoses is clearly protected by privacy. We can also include as part of the definition of personal information any information conveyed by an individual or used by a physician in diagnosing a case of PTSD, such as a patient suffering from intrusive thoughts or images, vivid flashbacks, feelings of nausea, or profuse sweating. But with the use of big data, what counts as personal information suddenly, and potentially dramatically, expands, as unconcealable and otherwise non-obvious factors such as speech patterns must now be considered as sensitive personal information. Those researchers who developed the AI that can detect PTSD were surprised at the patterns that the AI discovered and relied on, as they seemed counter-intuitive to what the researchers predicted would be relevant (Coleman 2019).

In response to the blurring of different categories of information, innovative accounts of inferential privacy are being developed, which can be described as a 'right to reasonable inferences', or a right to protection against inferences drawn through big data analytics that may cause reputational damage or have low verifiability (Wachter & Mittelstadt 2019, p. 580). The right of inferential privacy is a step in the right direction regarding the usefulness of privacy, but as Wachter and Mittelstadt rightly observe the development of such a right will require new policy mechanisms that focus on the consequences of the use of data rather than on the obtaining of data (2019, p. 580). While there may not be an absolute right to inferential privacy, particularly if we accept that information released publicly loses the protection of privacy and the prevalence of inferential reasoning about others in everyday social interactions (2018, p. 219), a qualified right to reasonable inferences, that is a right to know and correct certain inferences would be an important part of any privacy-based framework of protections.

However, inferential privacy still cannot adequately provide protection from harm because inferences might be drawn that are not clearly unreasonable while still leading to harm. Take for example the kind of inferences that may be made about a job applicant through big data driven screening processes, where the end result is that individuals are discriminated against based on disability (O'Neil 2016, p. 106). The inference that the algorithm produces may not, and indeed probably would not be, that person X has disability Y. It is much more likely that the inference would be that person X is not suitable for this workplace, and that is harder to detect as unreasonable because the inference is not a clear-cut statement of personal information. Ultimately, privacy as a rights framework is focused on individual rights to the protection of personal information, and as the category of personal information becomes blurred, even if the protection is focused on the output (the inference), it cannot capture every scenario.

The core assumption of privacy is that we can distinguish between personal and non-personal information, but the use of big data means that we can no longer clearly say what is not personal information. In those contexts where big data is used to infer personal information, we often do not or cannot know what information will be useful for inferring personal information. Increasingly, nearly every piece of information may be potentially personal information for the purposes of privacy, and as such the concept of privacy can no longer function alone in the face of big data. This is the heart of the inference problem, and the challenge posed by big data.

Conclusion

Ultimately, the concept of privacy cannot alone cope with how big data-based technologies function. The attempts to update privacy to cope with the digital age are in a way just another step in a long history of privacy being revised and updated in response to the development of new technologies. But big data presents a novel challenge through the inference problem. Privacy is still a valuable concept, and I am not arguing here that we should abandon privacy completely. In more traditional situations, contexts, or realms of the infosphere, such as the doctor’s office, the priest’s confessional, the office board room, or family home, a privacy-based approach is still appropriate, as we are concerned in these situations with the movement of information between individuals and around the environment and we can clearly identify the relevant personal information to protect. There are also some privacy-based solutions that may be relevant to the use of big data. The newly emerging inferential privacy shows promise for adapting existing privacy protections for the context of big data.

However, big data still presents a problem for the assumptions that lie at the heart of conceptions of privacy. Big data allows for the inferring of personal information and identity in ways that sidestep privacy, and problematise our understanding of what personal information is. The minimal conditions for the operation of privacy is that we can identify specific personal information to protect, and that we can protect those pieces of information. Big data blurs these conditions such that we can no longer rely solely on the tools that privacy-based frameworks offer. As a result, we must look to other conceptual frameworks for the appropriate tools to replace or supplement to tools of privacy, and one such framework is the nature of power.

Chapter 3

Power

I have argued that we should be sceptical of the claim that privacy rights can be updated or reformulated in some way to protect the interests of individuals in the face of big data. If we can no longer solely rely on privacy, we must look for other lenses to view big data through. Privacy rights have traditionally been concerned with how people can be harmed by the misuse of information, such as through unfair discrimination based on sensitive personal information or injuries to autonomy from the misuse of personal information. It is largely because privacy is concerned with the misuse of information that it has seemed like the most suitable tool to protect people from data related harms. However, as shown in the previous chapter, we cannot solely adopt a privacy-based strategy to meet the challenges presented by big data. We need an additional theoretical framework to fill these gaps, which will in turn help us to design new legal and ethical protections.

The various technologies of big data radically change the ways in which information is used and processed. Big data driven surveillance allows the capture and analysis of huge volumes of highly granular information, which exposes people to unprecedented levels of scrutiny and control. Routine decision-making processes are being automated through AI and machine learning processes, changing the nature and our experience of authority. Many big data technologies also involve the construction of essentially new digital entities as representations of people and processes, and these digital entities are being increasingly targeted by exercises of power instead of the people and processes they represent. However, while the development of big data has led to information being used in new and radically different ways, we are still concerned with the same kinds of harms, such as unfair discrimination and the undermining of autonomy. In order to properly understand then how the use of big data can lead to these same harms, I contend that we need to examine the ways in which big data is used as a technology of power and how big data changes the means by which power is exercised. At first this may seem odd, as privacy is a normative concept, while power is not. But I argue that where privacy falters in the face of big data, we need to understand the operation of power to see how individuals are being harmed such as through the violation of normative concepts like equality and autonomy.

This chapter will set out what is necessary in order to rethink how power functions in the age of big data. The central argument of this thesis is that there is no simple, single answer to the question of "what is power in the age of big data?". Big data is not one single thing, it is an umbrella term used to refer to a wide range of technologies that can be used in a diverse range of contexts. Similarly, power is not one single thing, it is also an umbrella term that is used to cover a wide range of distinct phenomena in an extensive range of contexts. We must avoid overgeneralising and using a one-size-fits-all approach, so I will propose here an analytical framework that is useful for assessing the use of big data as a technology of power across a wide range of diverse contexts. As such, this chapter will present a pluralistic approach to the concept of power, and a series of focused questions that can be used in analysing the exercise of power across different contexts.

First, I begin with a critical examination of how the current literature treats the relationship between big data and power. Several theorists take the view that the development of big data necessitates a new understanding of power, a kind of "big data power", which explains how power has been transformed in the digital age. However, I argue that such an approach is misguided. The concept of power is better understood in a pluralistic sense, much like big data. Big data is an umbrella term for a range of technologies, and likewise we use the word power in a diverse range of contexts to refer to an equally diverse range of phenomena. The concept of power resists definition in a unitary and comprehensive way, and as such we need to examine the relationship between modes of power and the specific technologies annexed to those modes of power.

Following this, I will set out a brief summary of several canonical accounts of power. Given the vast literature on power, this summary does not attempt to be comprehensive or complete. Rather, I highlight some key features that are important for the project of this thesis from the theoretical accounts of seminal writers such as Hobbes, Dahl, Weber, and Foucault. From this discussion I develop a rough taxonomy of types of power, grouped into 'causal', 'procedural' and 'productive' conceptions of power. This taxonomy is used in subsequent chapters to examine how big data is variously used to amplify and extend the exercise of power in different contexts.

Finally, I will show how we can use a pluralistic attitude towards power to identify different modes of power, that is different forms or expressions of power, within different contexts. This analysis draws on Floridi's method of levels of abstraction (Floridi 2002, 2008, 2014b), where the level of abstraction at which our investigation is placed determines the relevant questions to ask. Instead of merely asking "what is power in the age of big data?", we should instead ask the more focused question "in this context, who is doing what to whom for what outcome?". This broader question can be broken down into four smaller and targeted questions, namely "what is the intended outcome of power?", "who is exercising power?", "who is power exercised on?", and "how does this power function?". By asking these questions, we can identify key contextual features of the context we are investigating that help us pick out the goal, agent, subject, and means of power within that context. From there, those key contextual features will guide us in identifying which key conceptual features of different accounts of power are present. This allows us to understand the operation of power within that context with more precision than by asking the more ambiguous question of "what is power?".

Power and Big Data

The relationship between technology and power is well recognised in the literature, beginning with Lewis Mumford in 1964 who argued that technology impacts on the distribution of power in society, and Langdon Winner in 1980 who built on Mumford's claims and argued that technology embodies forms of power and authority (Sattarov 2019, p. 2). Beyond simply embodying or distributing power, the development of a new technology will often change how power operates. New technologies bring with them new capabilities, and these new capabilities will necessarily impact on the operation of social power (Kirkpatrick 2008, p. 5). Foucault's influential writing on the nature of power (Schirato et al. 2012, p. 53), for example, is in many ways a detailed examination of how new forms of power develop over time in response to the development of new technologies and sciences.

As part of this work on the relationship between technology and power, there is a growing group of writers who are turning to the more specific question of the nature of the relationship between big data and power. While the development of big data has certainly led to radical and revolutionary changes in society, the focus on the revolutionary nature of big data has led to the literature adopting a general approach of searching for the one account of power that best explains the relationship between big data and power. We can roughly divide these writers into two categories. The first group are those who argue that the development of big data has driven a shift from a Foucauldian disciplinary society towards a Deleuzian control society. The second group more radically argue that the development of big data necessitates the development of a whole new kind of power to accompany it. I will now examine these views in more detail, before arguing that these approaches are fundamentally mistaken.

Cheney-Lippold (2011), Thompson (2016), and Matzner (2017), are all examples of members of the first group of writers, who variously argue that big data has led to a shift from a Foucauldian disciplinary society to a Deleuzian control society. Cheney-Lippold (2011) argues that the way that big data can be used to categorise individuals suggests we need a Foucauldian analysis of power, but that the idea of disciplinary power is now outdated. Discipline prefigures how an individual can interact with the world through shaping normative discourses, but Cheney-Lippold argues that big data operates by modulating individuals and subjecting them to a constantly shifting cast that creates and re-creates the individual constantly and rapidly, just as with Deleuze's construction of control.

Thompson (2016) argues similarly to Cheney-Lippold that the ways in which big data can be used to categorise individuals has led to a shift to Deleuzian control away from Foucauldian discipline, and this can be seen in the use of big data in school systems. For Thompson, while discipline relies on constant surveillance such as through the administration of exams, control relies on rapid testing. Examination and testing regimes administered in schools under a disciplinary regime are pre-figured, in that there is a pre-determined norm that is being pursued. To pursue this norm, students sit the same standardised test, which then assesses how successfully those students have been trained in line with the pursued norms. But big data allows for Computerised Adaptive Testing, or CAT, where students are assessed by non-standardised tests (Thompson 2016, p. 830). These tests rely on algorithmic processes that assess the abilities of the students and present them with questions tailored to their current education levels. These assessments, according to Thompson, are good evidence of the shift from a disciplinary society to a control society, as testing in education no longer requires standardised tests and grading but can instead operate through rapid and algorithmically determined examination to create personalised profiles for each student.

Finally, Matzner (2017) argues that a Foucauldian perspective on big data is highly instructive, as big data can be used to subjectivise individuals, but the rise of big data has completed the shift from discipline to control. A key feature of Foucault's account of power is constant and uninterrupted surveillance. This surveillance captures data from individuals and is then used in processes to train them to be idealised subjects of power. Big data, which involves the mass collection of data from people, is an ideal method for this kind of subjectivisation (Matzner 2017, p. 32), as huge volumes of data can be collected and analysed rapidly. However, this also brings about the shift towards a control based society and away from a disciplinary society, as this collected data is not used to train individuals according to some predetermined norm based on the needs of a given institution, but instead to divide them up and foster competition (Matzner 2017, p. 31). The individual is divided into a mass of data points that can be moved, recombined and examined to create different pictures of the individual, nudging those individuals to continuously train themselves and compete with others rather than be trained towards a single coherent norm.

The second group of writers are those who see big data as being so transformative a force that it requires the construction of an entirely new account of power. Here I will briefly describe some of the main elements of each account. Rouvroy (2016; 2013) proposes an account of big data driven power she calls 'algorithmic governmentality'. Algorithmic governmentality refers 'very broadly to a certain type of (a)normative or (a)political rationality founded on the automated collection, aggregation and analysis of big data so as to model, anticipate and pre-emptively affect possible behaviours.' (Rouvroy & Berns 2013, p. 173). The development of big data facilitates a shift away from Foucauldian biopolitics and towards algorithmic governmentality because the operation of big data is not concerned with supporting, reinforcing, or multiplying life in the way that Foucauldian biopolitics is (Rouvroy 2016, p. 33). Where power as Foucault describes it subjectifies individuals to govern and manage their lives and ensure the health of the populace, Rouvroy argues that big data operates to avoid subjectivising individuals and is entirely unconcerned with managing the lives of individuals. This difference means that we have left Foucault's account of power behind and entered an age of algorithmic governmentality.

Han (2017) takes a similar approach. Where writers like Cheney-Lippold, Thompson, and Matzner argue that there are useful elements of Foucault's work that can be combined with Deleuze's work on control, Han argues that Foucault's account of biopolitics is dated and stuck in the 18th and 19th centuries. According to Han,

> *Foucault evidently did not appreciate that biopolitics and population – which represent genuine categories of disciplinary society – are unsuited to describing the neoliberal regime. Consequently he failed to do what the circumstances actually called for: to make the turn to* psychopolitics. (Han 2017, p. 19, emphasis in original)

For Han, Foucault's work is historically and geographically tied to a specific period of European history, and as such is no longer the organising "force" behind contemporary society (Han 2017, p. 19). The replacement then, according to Han is psychopolitics, an analogue of Foucauldian biopolitics. Where biopolitics tracks physical statistics about the population, such as health, birth rates, and death rates, psychopolitics tracks non-physical data, such as emotions, desires, and dispositions. Normally this information is hard to track, but big data driven analysis makes it possible to capture and track this information across larger populations. Just as biopolitics is an essential part of disciplinary power, Han's account of psychopolitics is an essential part of what he calls smart power, a kind of power that works by quietly guiding or encouraging an individual to subject themselves to power, rather than coercing or training them.

Beer (2016) proposes an account of metric power. Put simply, to exercise metric power is to use metrics or measurements of the world (and in particular of individuals) to shape and influence human decision making (Beer 2016, p. 177). For Beer, modernity is marked by a desire to measure and capture the world around us, including the lives of individuals, and the development of big data has allowed this desire to operate essentially on overdrive. As masses of data are collected, they render things visible or invisible in the eyes of those wielding power, and orders and categorises those who may be affected by the operation of power. These metrics then prefigure judgements, allowing those who wield power to shape and influence the decisions of others.

Finally, Zuboff (2019), as part of her work on surveillance capitalism, develops the idea of instrumentarian power. Zuboff defines this kind of power as ‘the instrumentation and instrumentalisation of behaviour for the purposes of modification, prediction, monetization, and control.’ (Zuboff 2019, p. 331) In other words, it is the rendering, computation, and most importantly the orienting of human experience for the purposes of the surveillance capitalist. Within surveillance capitalism, data is capital, and so a primary method for capitalists to ensure maximisation of profits within this system is to collect as much data as possible. Once this data is collected, it can be used to predict and then modify the behaviours of individuals to reduce the risk the capitalist is faced with and to increase potential profits even further. Power then functions here by nudging and manipulating the actions of individuals to make the predictions made by the capitalist self-fulfilling. While each writer in this second group develops a different account of the relationship between big data and power, the commonality of their approaches is that they understand big data as leading to the development of a kind of “big data power”.

Both groups in the literature, namely those who argue that we need a Foucauldian analysis of big data and those who suggest we need an entirely new account of big data power, are ultimately making the same mistake. That mistake is that they are searching for a kind of master concept or understanding of power; one theoretical account that explains the relationship between big data and power. For those in the first group, the error is in looking for a single account of power that explains what power is in the “big data age”. While it may certainly be true that aspects of contemporary society may be better explained by Deleuzian notions of control than by Foucauldian notions of discipline, this is not true of all the many different technologies that make up big data. When we pay attention to the variety of uses of big data, it is clear that any single account of “the” relationship between big data and power would be an oversimplification.

For those in the second group, the error lies in too tightly conflating the development of a new technology with the development of a new form of power, such that the new technology is in a way constitutive of a new form of power. Again, while the development of a new technology will often impact on how power is exercised, big data describes a diverse range of technologies that augment different forms of power in different contexts. As such, the development of big data cannot be seen as constituting a new form of power, because there is no single new big data technology or form of power.

The best way forward is to adopt a pluralistic approach to the concept of power and treat it as an umbrella term much like the term big data. While the writers considered above do not explicitly consider such an idea, there is already implicit support for this kind of approach in their writing. For example, Matzner suggests that there may be contexts in which different kinds or forms of power overlap, such as in an airport where some travellers will perform Deleuzian self-control to make it easier for them to travel with ease while others will be subjected to Foucauldian discipline and have themselves trained and normalised through disciplinary measures (Matzner 2017, p. 34). Other writers such as Zuboff (2019) and Thompson (2016) examine the operation of power within specific contexts, namely the structuring of economic systems and schools respectively, leaving it open for these and other approaches to power to co-exist. This is the approach we should take, as we abandon the search for the one true account of power, and instead take a pluralistic approach that recognises the many different ways in which big data can be used as part of exercises of different forms and kinds of power.

A Taxonomy of Power

Just as big data is not a single technology, power is not one single thing. As Dahl (1957, p. 202) aptly describes it, the word power is an 'awkward word', in that it has no convenient verb form, nor does it supply nouns for those who wield and those who are subjected to exercises of power. While these grammatical issues certainly do contribute to part of the awkwardness of the word power, there is another more important way in which power is an awkward word, stemming from how much we use the word power. "Power" is an immensely flexible word and concept, and we use it to refer to a huge and diverse range of social, political, and economic phenomena. Attempts to define power are fraught with difficulty, which is clear in the long history of the philosophical project devoted to this end. Yet, despite this difficulty, we have no trouble using the word as part of our everyday language, confidently pointing to a huge number of phenomena and saying that "that is power".

For example, we use the word power in the context of international relations and diplomacy between nations and in the context of parents making decisions for their children. We see power in politics, economics, schools, personal relationships, and individual actions. We have power that exists within the relationships between individuals, between groups, and between individuals and groups. There is power that is formal and power that is informal, specific and precise or generalised and diffuse. There is power whose scope and means are clearly delineated, for example a teacher has power over their students within the confines of the classroom but has no power over their students at home, and power whose scope and means are not clearly delineated, for example a general power to take another's possessions by force. Power comes from one central point, from many diffuse points, from human agents, from architecture and the environment, from possessions and/or personal characteristics. Power operates from above and can operate from below. It can be exercised through the threat of physical force, the operation of detailed surveillance, or from complicated social norms. It can come from personal strength or arise from positions of legitimised authority.

Just based on the way in which we use the word power, any attempt to develop a unitary account of power is impossible. The concept of power is broad, and as detailed above is used in such a broad range of contexts to refer to many different phenomena. Any attempts to provide a single explanation of power across these differences will be conceptually unwieldy at best, and impossible at worst. I propose that we can adopt a pluralistic attitude towards power as a theoretical lens that allows us to avoid these problems. Once we become sceptical of the notion that we can develop a unified theory of power, we can instead move on to a broader and more practical understanding of power. In short, as we use the word power within a range of different contexts to describe a range of phenomena, in order to properly understand how power works within a given context we must use an account of power that is fine tuned for that context. To do so, we need to develop a kind of taxonomy of different types or kinds of power that focus our attention on the specific mechanisms, power relations, forms of authority/influence/force etc which are relevant for the context we are examining.

My approach here is not to propose a new ontological framework of power. I am not arguing that there are, as ontological facts, *X* number of ways of doing power, and that we must select from this list for any context that we are studying. I am also not proposing to develop a new account of power which then contains several different forms of power. The approach I am proposing here is to instead recognise that certain influential theories of power are not actually straightforwardly opposed to each other, indeed within different contexts they may overlap or operate in parallel with each other. They are instead drawing out different domains or contexts in which power operates, and what makes them seminal accounts of power is that they are the first or the most influential accounts of how power operates in a context. The pluralistic approach to power is a recognition that in developing these different accounts of power, each writer is setting out the central characteristics or features of how a certain kind of power functions. As such, rather than raising theoretical disputes between different authors, the approach here is to pay attention to the contexts that they are investigating and the specific features of their accounts such as structures, relationships, technologies, techniques, etc. that are characteristic, or the primary theoretical innovations, of that account of power. I will go into more detail about the questions we can ask to identify a mode of power later in this chapter, but what is necessary to spend some time on now is a kind of taxonomy of seminal accounts of power.

Power, as a philosophical concept, has a long and extensive history in the academic literature. It is a major concept in philosophy and a foundational concept of sociology and political science. Beyond academic inquiries, as individuals we have many intuitions about how power operates (Morriss 1987, p. 1). Indeed, we interact with power daily: we exercise power, are subjects to power, exist in networks of power relations, and otherwise see and feel power. Yet the essential nature of what power is and how it operates is ‘an essentially contested concept’ (Gallie 1956), whose definition is bound to various value-assumptions that predetermine its application (Lukes 2005, p. 30). As such, within the academic literature we find a wide range of different forms and kinds of power being identified and dissected.

What follows here is a kind of synoptic taxonomy of different theoretical accounts of power which will be useful over the course of this thesis. I have grouped the accounts considered here into three rough categories, namely causal, procedural, and productive accounts of power. Causal accounts of power characterise power as a causal force and are primarily concerned with the end effects of an exercise of power, while procedural accounts characterise power by the rules and processes through which power can be exercised, and as such are primarily concerned with the ways in which power is exercised. Productive accounts of power are those accounts that see power as a force that shapes and moulds the people it is exercised on, and these accounts are primarily concerned with the ways in which that shaping, or moulding, takes place. This is not an attempt at an exhaustive history of power, which would require a whole thesis in and of itself. This is, instead, a rough way of categorising several theoretical accounts of power in ways that bring out their key conceptual features and innovations. This in turn will be a useful and instructive tool to draw on when thinking about how big data technologies can be used by different kinds of power, and how the exercise of power is changed or impacted by the use of big data.

Causal Accounts

In a causal account of power, power is understood as a causal force. Power is either what is necessary to cause a certain state of affairs to come into being, or power is the act of causing some state of affairs to come into being. Typically, in a causal account of power, power is construed as a thing that can be possessed, i.e. what is necessary for the operation or exercising of power can and must be possessed by the person who is attempting to exercise power. This possession can either be a personal characteristic such as charisma or strength, some material possession such as wealth, or be derived from a specific position or station. Then, by using these possessions, someone can exercise power. Additionally, the end effects of an exercise of power are an important part of a causal account. Those writers who develop causal accounts of power are often primarily concerned with these end effects, as observing them can be useful in detecting successful exercises of power. I will look at three seminal causal accounts of power, firstly Hobbes' approach to power and Sovereignty, Dahl's empirical account of power, and Lukes' three-dimensional account of power.

Hobbes

Many trace the development of causal accounts of power back to Hobbes (Clegg 1989, p. 25), who argued that 'Power and cause are the same thing' (Hobbes 1839, p. 127). For Hobbes, to say that an agent has the power to produce some effect is to say that an agent has what is necessary for causing that effect. Where contemporaries of Hobbes such as Suarez argued that freedom is a form of power, i.e. that freedom is the power of the individual to do something or refrain from doing something (Martinich & Hoekstra 2016, p. 173), Hobbes instead positions freedom as the absence of external obstacles to the ability of an agent to cause desired effects from coming about (Martinich & Hoekstra 2016, p. 183).

Building on his causal account of power more generally, in *The Leviathan* Hobbes looks at how power is wielded by individuals, and states 'The power of a Man, (to take it Universally,) is his present means, to obtain some future apparent Good.' (Hobbes 2018, p. 76). Hobbes then goes on to list several forms that power can take and the ways in which it can be wielded. Power, as individuals can use it, can be roughly grouped into two categories, namely natural and instrumental, whereby natural power arises from personal characteristics such as strength, form, eloquence, or nobility, where instrumental power is derived from external things such as fortune, reputation, or position. Hobbes is largely quiet on how natural and instrumental power cause future Goods to come into being. However, from his construction of natural and instrumental powers, we can see that natural powers largely function directly, such as through physical force or direct persuasion, while instrumental powers will often rely on reputation to induce a change in behaviour. Whether the source of power be natural or instrumental, for Hobbes it is a causal force, through which individuals can obtain a future 'Good', or otherwise satisfy their desires and intentions.

For Hobbes though, the purest expression of power was in the rights of the Sovereign. Hobbes' innovation in political theory was his approach to the Sovereign, which he described as not arising from an agreement of a society to organise into a state, but instead as arising from people coming together and agreeing to let one person, the Sovereign, make binding decisions. The Sovereign, a kind of artificial person constituted through essentially the handing over of power by the population, had a first line of power whereby they had the right to authorise certain acts and define what was peaceful and what constituted a threat to the stability of the State, and reserve powers to make others desist or refrain from actions that were unauthorised (Clegg 1989, p. 28). The Sovereign was thus both a stabilising force, and a source of fear, for the Sovereign had the right to decide that a particular individual or group constituted a threat to the stability of the State, and once decided, could then effectively "declare war" and threaten the use of State force to protect the State.

Hobbes also notes that power is 'like the motion of heavy bodies, which the further they go, make still the more hast.' (Hobbes 2018, p. 150). Power in a way begets more power, particularly for power borne from instrumental sources such as fortune, reputation, or position. As power is exerted and those individuals who exert power obtain their desired ends, they will often end up with a greater source of power than before. This works in much the same way as a boulder gathering a momentum rolling down a hill, or using money gained through investment to invest further and increase returns on and on. As power is exerted, it can increase in strength, and those individuals exerting it can have a greater causal impact on the world around them.

Dahl

Dahl's account of power has become hugely influential in the literature, and his definition 'A has power over B to the extent that he can get B to do something B would not otherwise do.' (Dahl 1957, pp. 202-3) is widely cited as a canonical definition of power in both philosophy and sociology. As a political scientist, Dahl was primarily interested in setting out a way to empirically measure the exercise of power in political frameworks. He was critical of existing accounts of power, particularly those of Aristotle, Hobbes, Machiavelli, and Weber, because they either failed to fully elaborate on the different terms of power such as power, influence, and authority or because they were too specifically interested in one particular term of power (Dahl 1986). As a result, he set out to try and develop a more general conception of power in political systems as part of the social relationships that make up such a system, with a strong focus on counterfactual analysis.

Power for Dahl is relational, in that it can only operate through social relations between actors, both individuals and groups. As part of this relationship, one actor will exercise power on another by acting in such a way that they cause someone to then act or refrain from acting in ways they would not without the intervention enabled through the social relationship. In this way, power is a causal force, for without the exercise of power the secondary actor would not act according to the wishes of the primary actor, and we can discover the operation of power through counterfactual reasoning. Crucially, this social relationship must involve conflict. The wishes of one party must conflict with the wishes of another, else any attempt to perform a counterfactual analysis of power will fail.

Dahl sets out four primary characteristics of power (Dahl 1957, p. 203):

1. Base – the source of someone's power. The base is made up of the resources that can be exploited as part of exercising power, including opportunities, actions, and objects.
2. Means – the methods by which the base of power is mobilised. This is a broad category, and can include such varied things as making a threat or promise, holding a conference, exercising charm, or performing certain actions
3. Scope – the responses of *B* to *A*'s exercise of power. In response to an exercise of power, the actor(s) who have power acted on them will have a range of responses available to them.
4. Amount – a probability statement of how likely power will be successful. For example, 'the chances are 9 out of 10 that if the President promises a judgeship to five key Senators, the Senate will not override his veto.'

From these four characteristics, we can then measure power as the probability that the actions of *A* will influence the actions of *B*. To illustrate, Dahl gives the example of a student reading the novel *The Great Transformation* (Dahl 1957, p. 204). There is initially a one in a hundred chance that James will read the novel over the summer holidays, but then his teacher tells him to read it for fun. If the chances remain at one in a hundred, there is no exercise of power. But if his teacher tells him to read it or he will fail the course, and the chances increase to 99 in a hundred, then we can say that the teacher has power over James. That is, the teacher has the base of passing or failing James and the means of power in making the threat of failing him, the scope of actions available to James are to read or not read the book, and the amount in the second scenario is high in that James goes from a low chance of reading the novel to a high chance of reading the novel.

Lukes

Lukes develops what he calls a three-dimensional account of power. For Lukes, the core or primitive notion of power is a causal notion, that *A* in some way affects *B* in a significant or non-trivial manner. Or, in other words, '*A* exercises power over *B* when *A* affects *B* in a manner contrary to *B*'s interests' (Lukes 2005, p. 37). This conception of power is directly inspired by his critique of elements of Dahl's account of power. Lukes' argues that Dahl's account is too focused on the idea of conflict, and that it relies on observing behaviour to detect the exercising of power (Lukes 2005, p. 17). This leads to Dahl falling foul of the 'exercise fallacy', where power is reduced largely to its exercise and can only be detected through the observation of direct conflict (Lukes 2005, p. 70). As a result, it becomes difficult to notice attempted exercises of power, and impossible to detect exercises of power that operate in more subtle ways i.e. without overt and observable conflict. Despite his critiques though, Lukes still sees Dahl's account as a valuable and useful account of power, and labels it as one-dimensional, or the first dimension of Lukes' three-dimensional account. When looking at exercises of power that fit into this first dimension, the relevant interests of each party can be broadly understood as policy preferences, or end desires for states of affairs, and through some conflict one party has their policy preferences prevail and others must change their actions in response.

For the second dimension, Lukes looks to Bachrach and Baratz, who similarly develop an account of power in reaction to Dahl. Bachrach and Baratz argue that Dahl's account is too restrictive, and we should also include as power situations where *A* creates or reinforces social practices that prevent *B* from bringing an issue forward if that issue is not in *A*'s interests (Lukes 2005, p. 20). So, we should see those situations where *A* directly causes *B* to do something as power, but we should also see situations where *A* manipulates, controls, or shapes social practices that in turn act as barriers to *B* even bringing up their interests as power. This kind of power operates through systems that encourage or force individuals to suppress or ignore their own interests as a result of social systems around them. While Lukes feels this is an improvement on Dahl's account and should be counted as a second dimension of power, it is still overly reliant on the idea of conflict. While it includes situations where the conflict is now non-obvious or covert, it still requires there be a measurable conflict between the interests of the various parties in a social relationship. The second dimension broadens out power to include non-decision making in governance alongside policy preferences but does not capture the whole story of causal power according to Lukes.

The third dimension of power that Lukes proposes is where *A* exercises power on *B* not just by making *B* suppress their own interests, but by shaping or determining what *B* feels their interests are (Lukes 2005, p. 27). This third dimension operates through preventing grievances rather than by having opposing interests directly conflict, a process that Lukes refers to as 'latent conflict'. Those who are affected by exercises of this third dimension of power may not even be aware of the operation of power, as their perceptions and cognitions are influenced such that they accept the operation of power as a kind of natural status quo, even though power is being exercised in the interests of the wielder of power. In this way, the third dimension of power covers those situations where interests are made silent through reinforcement of the status quo, as those who are subjected to power adopt the interests of the wielder of power as their own. There is no direct or even indirect conflict in these situations, as any conflicting interests are discarded, often sub-consciously.

While Lukes differentiates his account of power from Dahl's by expanding the notion of power through the addition of multiple dimensions, he still presents a causal account of power that operates in social relationships and is best examined through counterfactual analysis. Lukes largely retains Dahl's counterfactual methodology, though he recognises that the construction of a counterfactual surrounding whether *B* would have thought differently had *A* not acted is more difficult than assessing *B*'s actions (Lukes 2005, p. 44). Because of this, Lukes' account is still a paradigmatic example of a causal account of power, as it is focused on the end effects of the exercise of power, even though he broadens out power to include situations with indirect and latent conflict.

Procedural Accounts

In this second category of accounts of power, procedural accounts, the theoretical focus is on the procedures or processes through which power operates or is exercised. In these accounts, while an exercise of power will still have an impact on the world, such as the alteration of behaviour, the focus is not on the causal impact of power. Rather, power is understood as a procedure of some kind, a set of steps that must be performed, and the performance of these steps or procedures is the performance of power. While a causal analysis of a tennis player hitting a tennis ball will focus on how the player causes the ball to move in a certain direction, a procedural analysis will examine how that player acts through modifying their arm movement, strength, stance, wrist angle, etc. in order to hit the ball in a precise way towards a desired area of the court. Similarly, a procedural account of power looks to explain how people perform certain procedures, processes, or rituals through which they can exercise power. Here I will briefly set out three influential writers who develop procedural accounts of power, starting with Machiavelli's pre-modern account of power as the successful use of strategy or tactics. From there I will look at Weber's account of bureaucratic power, and then at Parsons' account of social power.

Machiavelli

We begin here with Machiavelli, who approaches power as a form of strategy rather than as a causal force (Clegg 1989, p. 31). For Machiavelli, we cannot understand power without examining what are essentially the moves in the giant game of strategy that is life. Even broader myths around the nature of power, such as Hobbes' myth of the Sovereign, are just more moves that can be made as part of the political games in which power is exercised. Much of Machiavelli's work on power is set out in *The Prince*, where he sets out a practical guide on how a prince may gain and keep hold of power within the court. At its simplest,

> *Power is simply the effectiveness of strategies for achieving for oneself a greater scope for action than for others implicated by one's strategies. Power is not any thing nor is it necessarily inherent in any one; it is a tenuously produced and reproduced effect which is contingent upon the strategic competencies and skills of actors who would be powerful.* (Clegg 1989, pp. 32-33)

We can measure power through the interplay and conflict between different strategies and tactics, each of which are attempts by individuals to exert power on others around them. Power here is not based on any characteristic of an individual, nor on any possession they own or have at their disposal. To wield power is to successfully execute a strategy to secure a greater scope of action over others. Executing a strategy is the same thing as doing power.

As to what these strategies are, Machiavelli does not present an exhaustive study, and indeed there will likely be many strategies possible today that were not available at the time. The basest strategy of power is the threat of violence (Clegg 1989, p. 33). While excessive violence may not be the surest long-term strategy for retaining power, threatening or carrying out violence against another is at the core of power, and many other strategies of power will either boil down to or otherwise draw on this central core of power. An example of a more complex strategy that Machiavelli recommends is for a prince to increase his renown and respect by becoming a patron of the arts to demonstrate his character. Across these various strategies, we can see that for Machiavelli power is not a personal capacity or that it arises from any particular point, but instead power is wielded as individuals act out strategies against each other.

Central to Machiavelli's conception of power is a competition between parties, as well as the possibility of winning. No one exercises power in a vacuum, there will always be conflicting and competing exercises of power as people struggle to secure a greater scope of possibility for themselves. As such, with Machiavellian power there will be an ultimate winner, or winners if a group works together, whose strategies will be more successful than their opponents and who will secure a greater scope of action for themselves. Power is then also comparative, in that we can directly see one person (or a group of people) with greater power than others, as different parties have differing success in their strategies and the breadth of the scope of action they secure for themselves.

Weber

The next account considered here is Weber's early 20th century account of bureaucratic power. Firstly, Weber broadly defines power as 'the probability that one actor within a social relationship will be in a position to carry out his own will despite resistance, regardless of the basis on which this probability rests.' (Weber et al. 1978, p. 53). Power is then 'amorphous' and can take many different forms, however the form of power that Weber is most concerned with is "domination",[3] which he defines as 'the probability that a command with a given specific content will be obeyed' (Weber et al. 1978, p. 53). Unlike Machiavelli, who avoids giving such a clear statement of a definition of power, Weber is somewhat closer to a causal account of power, especially in how he constructs power and domination. At a later point, he says that domination is successful if it alters the conduct of another 'as if the ruled had made the content of the command the maxim of their conduct for its very own sake.' (Weber et al. 1978, p. 946). Just as in Dahl's approach to power, in order to spot power, it is necessary to see where an individual alters their conduct as a response to an operation of power.

However, Weber's account is better understood as a procedural account of power because domination, especially domination of large groups of people, needs to be legitimatised (Weber et al. 1978, p. 213). Weber proposes three main bases of legitimacy for power, the important one here

[3] The word Weber uses is *Herrschaft*, which does not have an easy English translation. It has been variously translated as 'imperative control', 'leadership', 'authority', or 'domination'. As to which is correct is not a major issue here.

being legal authority. Where domination is legitimised by legal authority, obedience is not owed personally to the individual(s) who are looking to dominate others, but instead more broadly to a rules-based system in which that domination can occur (Weber et al. 1978, p. 216). A system of legal authority, as Weber puts it, is a system of abstract rules, which are administered in processes specified by those same rules. Obedience to that system is only owed by those who are a member of that same system, and that obedience is not owed to a person in authority but more broadly to the system itself. So, a crucial feature of Weber's account of power is common membership in a system, as power cannot be exercised on someone in a different legitimising system to the wielder of power. Additionally, an exercise of domination then is only successful if it follows the rules and procedures set out in the system itself. In order to properly understand how domination functions, it is important to understand the rules and procedures that power must act through to be successful.

The purest exercise of legal authority for Weber can be found in the bureaucracy (Weber et al. 1978, p. 220). Within the organisation of the bureaucracy, the chief of the organisation has dominance within their specified sphere, and below them sits a hierarchy of officers who make up the staff of the "monocracy". Indeed, this kind of monocratic bureaucracy is the most efficient way to exercise authority and power over others – because of its grounding in rules and procedures, it has a high level of stability, precision, and stringency. In many ways the bureaucracy has become indispensable in modern life, both in political and economic spheres. The essence of the bureaucracy is domination through knowledge (Weber et al. 1978, p. 225). There are two types of knowledge essential for the operation of power in a bureaucracy. The first is technical knowledge within the relevant sphere, but the second, and arguably more important knowledge, is knowledge of the system itself. In order to operate power within a bureaucratic structure it is essential to know the rules and procedures of that system; to know how it is possible to wield power and exert domination within that system. Power in such a system only operates according to the rules and procedures of that system. To act in violation of those rules or to otherwise ignore them means that any attempt to wield power will ultimately fail.

Bureaucratic structures are widespread in modern society. While it is most common to think of bureaucracies in relation to government organisations, political parties, or other state institutions such as hospitals and justice systems, they are widespread outside of government (Weber et al. 1978, p. 974). The modern capitalist enterprise relies heavily on bureaucratic structures thanks to the unparalleled speed and precision the structure offers for production. Across society, especially recently, there has been trends towards objective and specialised administration in all areas of life, and it is objective and specialised administration that bureaucracies offer. As such, the power that comes from knowing the rules and procedures of the system that power can be operated through becomes even more important as bureaucracies spread and grow. So, while Weber presents a definition of power which has echoes of a causal account of power, it is grounded in knowledge of rules and procedures, and the operation of power is bound up in the correct application of those rules and procedures.

Parsons

A second prominent contemporary procedural account of power was put forward by Parsons. His account is motivated by problems he finds within the causal accounts of power (Parsons 1986, p. 95), particularly his concern that causal accounts reduce power to a zero-sum game. For Parsons, causal accounts construe power as a kind of limited resource, a system with a finite amount of power to go around. When person *A* exercises power over person *B*, *B* lacks the amount of power that *A* is exercising, and should *A* increase how much power they have, then others within the system must lose the corresponding amount of power in return. Parsons argues that in the real world, power is often more flexibly attributed across actors, without the need for a gain in power by one to be accompanied by an equivalent reduction in power of another. Instead, we should see power as the 'capacity for action in a society':

> *Social power is possessed by those with discretion in the direction of social action, and hence predominantly by those with discretion in the use of routines ... The possession of power is the possession of discretion* (Barnes 1988, p. 58)

To exercise power then, for Parsons, is to manipulate or control the opportunities and procedures of others within a social system. The individual who has power is not necessarily the individual whose strategies have been the most effective (though this is often the case), but instead the individual who has power has a degree of influence or control over the strategies and actions taken by others.

At the heart of Parsons' construction of power is an analogy between the concept of power and the concept of money (Barnes 1988, p. 14). Within an economic system, currency functions to secure the performance of obligations. The offering of money in exchange for a good or a service functions to secure the performance of the obligation to provide that good or service. The offering of money is not a cause of the performance of the relevant obligation, but instead works to ensure that performance. Power for Parsons works in much the same way. *A* can "spend" his or her power like a currency to secure *B*'s performance of some obligation. *A* has power over *B* not because *A* has the ability or right to cause some behavioural change in *B*, but instead *A* has the generalised right by virtue of the currency they possess and spend to secure *B*'s performance of a now binding obligation (Lukes 2005, p. 31). Interestingly, while we would still in these situations say that it is *A* who is powerful or has power as such, it comes to rely on the "powerless" for the performance of their obligations.

Parsons also distinguishes between 'primitive' and 'complex' systems of power, just as there are 'primitive' and 'complex' systems of money (Parsons 1986, p. 112). In a primitive system of money, the value of money is tied to some physical object. Commonly this object is something valuable such as gold or silver, and the value of a given unit of that currency is equivalent to a set amount of that physical object, such as an ounce of gold. However, in more complex monetary systems, currency is floated, released from any tie to a physical object, and their value is instead determined by supply and demand. A similar distinction appears in power according to Parsons. In primitive power systems, power is tied to physical force, or the threat of physical force, however in more complex systems power depends on authority and legitimacy. For Parsons, many examples of political and social power in developed countries are examples of this more complex form of ‘power-currency’, and the source of power is not the threat of violence but a sense of legitimacy coming from authority. It is these more complex systems of power that Parsons is primarily concerned with understanding.

In more developed systems of power, where power is legitimised through authority rather than through the threat of violence, Parsons suggests that there are four main strategies of power available, i.e. there are four methods with which someone can exercise power (Parsons 1986, p. 104). These four strategies can be categorised across two dichotomous variables: channel and sanction type. The two channels are situational and intentional: an individual looking to exercise power can do so by either attempting to control or manipulate the situation around another person, or by attempting to control or manipulate the intentions of another person such as through manipulating symbols that person sees as being meaningful. An individual looking to exercise power can then also offer one of two sanction types, positive or negative sanctions, as rewards or punishments for compliance with the exercise of power. The possible combinations of these two variables produce the four available strategies of power:

1. Persuasion – positive intentional – symbolic ‘reasons’ are expressed as to why an individual’s compliance with an exercise of power is advantageous to them;
2. Inducement – positive situational – the material situation of the individual being targeted by power is changed (at least presumptively) to the benefit of the target of power;
3. Activation of commitments – negative intentional – symbolic ‘reasons’ are presented to the individual being targeted to explain why noncompliance would injure their interests;
4. Coercion – negative situational – an alteration of the situation of the individual being targeted by an exercise of power where that change is detrimental to the target individual.

		Channel	
		Intentional	Situational
Sanction Type	Positive	Persuasion	Inducement
	Negative	Activation of commitments	Coercion

By undertaking these strategies, an individual can exercise power over another, and secure compliance with their wishes. While this is somewhat causal in nature, that is the exercise of power is aimed at causing an individual to comply with the wishes of another, the focus of the account is on the four legitimised strategies that can be employed to secure that compliance and on the way in which exercises of power control and limit the strategies and actions of others.

Just as with the various causal accounts of power, there are substantial differences between the various procedural accounts of power, but there are core similarities. While for Machiavelli power is wielded through the implementation of strategies and techniques, Weber describes a form of power in which knowledge of the rules and procedures of a system allows for the operation of power or domination. Parsons differs again and develops an account whereby an exercise of power restricts the opportunities and procedures that others can utilise. But across them all the primary focus of these accounts is on how power functions. To wield power is to follow a procedure, a set of steps or rules, through which power is activated and comes to bear on others.

Productive Power

The third category here is productive accounts of power, which is a much more recent development in the literature than causal and procedural accounts of power. The theoretical focus of a productive account of power is on the ways in which power shapes the identities of those who are exposed to power, either as its wielder or as its subject. In this way, the operation of power is not a causal force or the result of following a procedure, but a constitutive force in defining those who interact with power. The paradigmatic account of productive power can be found in Foucault's work, particularly in his work on biopower and disciplinary power. As such, I will only be considering Foucault's work here, though his writing is heavily influenced by Marx's work on false consciousness and is a key influence for Deleuze's writings on the society of control.

Foucault

Power, for Foucault, is relational in nature (Foucault 1988, pp. 94-95). That is not to say that there are specific kinds of power relations that we may enter into, or that within existing relationships there are layers of power over the top of them. Instead, Foucault argues that power is an inherent part of all relationships, and indeed power cannot exist outside of relationships. Power is the immediate effects of divisions, inequalities, and differences between the parties of a relationship, both defining the nature of that relationship and defined by the nature of that relationship. This is demonstrated clearly in Foucault's examination of the relationship between factory owner and employee. The factory owner is in a position of power over the employee not by virtue of their ownership of the factory nor because of any inherent character trait they possess that the employee does not, but as a result of the relationship that the two have with each other. Should someone else step into either role, the power relation between the two roles would largely remain the same because the nature of the relationship would also remain largely the same. These power relations are intentional and non-subjective, as 'they are imbued with calculation: there is no power that is exercised without a series of aims and objectives.' (Foucault 1988, p. 95). Power relations have meaning not from some external explanation, but because those relations are in themselves imbued with meaning arising from the aims to which those relations are aimed. Because power is inherently relational, Foucault also argues that resistance to power is an inherent part of the operation of power. As the functioning of power relies not only on those who are "powerful" but also on those whom fulfil the role of target or adversary, there can be no power relations without someone who might resist those power relations.

Importantly for Foucault, power is not exercised from a single point. Power is instead a kind of capillary force; it is a flexible force that is 'exercised from innumerable points' (Foucault 1988, p. 94). It is not something that can be held on to by an individual and used against others, it exists across the relationships that make up society, shaping the 'social body' as a whole. Power as a force is exercised from the nature of the relationships that give rise to it, and as Foucault argues also through the architecture and structures around us. In this way, power is almost an automatic process, a force that is continually being expressed in the relationships we enter and the world we move through. This is different from both causal and procedural accounts of power, as both causal and procedural accounts presuppose an individual or group actively exercising or wielding power intentionally, but in a Foucauldian structure of power it is more automatic and distributed. That is not to say that there is no intentionality behind power – as noted above, Foucault believes that power is 'imbued with calculation', it is intentional and non-subjective as it gains its meaning from the relationships through which power operates. What automatic means here is that it can operate without an active exercise of power by an authority figure.

Another important element of Foucault's approach to power which can be seen clearly in both *History of Sexuality* (1988) and in *Discipline and Punish* (1995) is that power is largely a productive rather than a repressive force. While of course there can be expressions of power which are overtly repressive, such as a slave-owner power relation, the essential nature of power is productive 'in the sense that it shapes and moulds people, their dispositions and values, and their practices' (Schirato et al. 2012, p. 46). As power operates it shapes those who are subjected to power relations into becoming more "normal" subjects. Within the operation of disciplinary power, those that are "disciplined" (e.g. prisoners, students, factory workers) are shaped over time into adopting the norms of the system such that they become better subjects for the power relations that they are subject to. For example, prisoners, especially those who inhabit the panopticon, through the operation of disciplinary power begin to self-regulate and to internalise the behaviours that power seeks to impose.

This productive effect of power is dependent on two other key features of Foucault's account of power. The first is what Foucault refers to as dividing practices (Schirato et al. 2012, p. 59). Within academic fields, there are systems of categorisation and taxonomies, much like the one being constructed here, that divide elements apart from each other and into groups. The operation of power relies on a similar process of division, as the criminal are divided from the law-abiding in the prison, the ill from the healthy in the hospital, and the insane from the mad in psychiatric clinics. As people are divided, they are then treated as a member of that category, and thus shaped over time to be ideal subjects of power.

The second key feature that largely enables the productive nature of power is a constant, and overt, surveillant gaze (Schirato et al. 2012, p. 88). For individuals to internalise the operation of power and to self-regulate themselves according to the power relationship they are in, a constant and overt surveillant gaze is crucial. Firstly, the surveillant gaze must be constant, or at least threatened to be constant. Those who are in positions of power in the relationship must be able to track those who are subject to power in order to gauge whether they are properly self-regulating, or at least they must be able to credibly threaten that the surveillance is constant. Secondly, as part of this threat, the surveillance must be overt. Those who are subjected to power must be aware that they are being surveilled, or else they would not begin to self-regulate. The panopticon is the paradigmatic example of the operation of power here, but it also extends to factories with oversight from managers, schools with exams and testing, and clinics with regular observations and charting. As those who are subjected to power and positioned in time and space within the network of relations, they are watched and they know that they are being watched (or at least that they could be being watched) at all times, and in response they self-regulate and discipline themselves as ideal subjects of power.

Modes of Power

To properly understand how power functions within a particular context, we must adopt a pluralistic attitude towards power, which is an attitude that recognises that writers who develop theoretical accounts of power are setting out what they perceive as being central characteristics or features of power that explain how power operates within a particular domain. I refer to these different 'operations' of power as *modes of power*, or a particular form or variety of power. A pluralistic attitude towards power provides a valuable theoretical lens with which to identify key conceptual differences and similarities between exercises of power within different contexts, or in other words to set out the mode of power in operation.

For example, it is clear that power operates and is experienced very differently for the subjects of a judge's decision in a court room, when compared with the struggle of a political election, and again when compared with the relationship between an employer and employee. In different contexts we see the operation of different kinds or modes of power and these differences need to be understood in relation to the different contexts in which they operate. It is important to note however that I am not claiming that within a context there is only one "mode" or kind of power present. The word "modes" here refers to different ways or means by which power can be experienced or expressed within a context and across different contexts. As such there are cases where multiple modes may be identified within a given context, possibly overlapping each other or perhaps even competing and conflicting with each other.

Such an approach avoids asking oversimplified questions, such as "what is power in the age of big data?" and asks more focused questions, such as "what is a specific exercise of power aimed at?", "who is impacted by this kind of power?", and "how does this kind of power use big data-based technologies?". An overly general conception of power may obscure important nuances and differences in the ways in which big data is used in exercises of power. Big data is not a single thing, it is a term that refers to a wide range of loosely related but importantly different technologies, and as shown above there is no one conception of power. Adopting a pluralistic attitude towards power helps us avoid getting trapped by simplistic questions and allows us to more precisely examine specific technologies and how they are used in different exercises of power. This is of vital importance as big data is increasingly used in wider varieties of decision-making processes across a growing range of domains and contexts, as an analysis which suits one particular context may at best be unsuited for another context, or at worse blind us to important aspects of other contexts.

Floridi’s method of levels of abstraction (Floridi 2002, 2008b, 2014b) provides a useful discursive tool for identifying the relevant modes of power. The central idea of Floridi’s level of abstraction method is that the level at which an investigation is placed will determine the relevant questions to ask, the answers obtained, and the affordances that can be made. The classic problem of Theseus’ Ship provides a good example of different levels. As Theseus’ Ship ages and decays, one by one each plank is removed by a master carpenter and replaced by a new one. Over time, more and more planks are replaced, until some point in time is reached where the entire ship is made up of replacement parts, and there is not an original plank or fitting left on the ship. At this point, is it still the same ship, or a new one? The correct answer, for Floridi, is not to say yes or no, but to ask, “who is asking, and why?”, to determine the relevant level of abstraction when the question is asked. A collector who is interested in the quality and originality of the ship would say it is not the same ship, while the tax office would say it is the same ship based on a continued ownership. Either way, questions about the same object results in different answers depending on the context and purpose of the questioner. (Floridi 2014a, p. 67). There is no one correct answer to the question “is this the same ship?”, the relevant answer depends on the relevant context the question is being asked in and understanding the correct level of abstraction allows us to reach the relevant answer.

Applying the ideas of the levels of abstraction here, our analysis requires asking the right questions. With Theseus’ Ship, the paradox is only present when we ask the ambiguous question “is this the same ship?”. The solution that Floridi gives us solves the paradox by simply avoiding it altogether. In asking the right question, we get a useful answer. So, when we ask “is this the same ship for tax purposes?”, we get the much more useful answer of yes, it is the same ship. The same is true for the pluralistic approach to power. Simply asking “what is power?”, or the equally unhelpful “what is power in the age of big data?”, gives us much the same answer as simply asking “is this the same ship?”. We need to ask more specific and focused questions in order to get useful answers.

What follows here is an initial proposal of four useful questions that can be asked when investigating a particular context. These four questions can help make clear key contextual features about the operation of power within a given context. We can then use those key contextual features to show us which conceptual features of different theoretical accounts of power are present within that context, or in other words what are the modes of power being exercised.

Asking the Right Questions

Just as with Theseus’ Ship, we need to be attentive to the key features and perspectives we are investigating when trying to determine the modes of power within a context. So, rather than simply asking “what is power in the age of big data?”, we must ask the more targeted question of “who is doing what to whom for what outcome?”. This question can be broken down into four sub-questions that guide the inquiry:

1. What is the intended outcome of power?
2. Who is exercising power?

3. Who is power exercised on?
4. How does this power function?

Goal

The first question to answer is “what is the intended outcome of power?”. The goal of an exercise of power is a crucial characteristic of a mode of power, and we can see the importance of the idea of a goal or aim across the literature on power. Many accounts of power explicitly view power as teleological in nature, and those that do not explicitly do so implicitly consider the importance of goals or aims for power. Indeed, the idea that power is always exercised in the pursuit of some desired goal is an intuitive idea. There seems to be little point in exercising power without some desired end goal in mind. Even those exercises of power which seem entirely capricious in nature, such as a king ordering his jester to dance, are being exercised with a goal in mind, even if that goal is just to enjoy the “feeling of being powerful”.

When Hobbes describes power as a man’s ‘present means to obtain some future good’ (Hobbes 2018p. 76), or when Machiavelli says that an exercise of power is the implementation of a strategy for a greater scope of personal action (Clegg 1989, pp. 32-33), it is implicit that the exercise of power is geared towards achieving a desired future good or goal of some kind. Dahl (1986, p. 39) and Lukes (2005, p. 34), who construct power as *A* getting *B* to do something that *B* would not otherwise do or contrary to *B*’s interests, require the reader to imply that what *A* is getting *B* to do is then something that *A* wants them to do, and Weber (1978, p. 53) links power to an individual carrying out their will despite resistance. For Parsons (Barnes 1988, p. 58), those who possess social power are those whose goals get met. Foucault’s approach to the concept of power is built upon the idea of it being useful for the pursuit of various goals, made clear in his exposition of disciplinary power and how it works to transform individuals into more compliant subjects of power.

More explicitly, there are some writers who have picked up on this general agreement on the goal-oriented nature of power. Galbraith (1984, pp. 9-10) describes power as ‘always purposeful’, in that it is always employed for some purpose, whether that be personal gain, community benefit, or even for its own sake as a form of personal enjoyment or fulfilment. Morriss (1987, p. 30), when examining how power can be successful or not successful, suggests that ‘To affect something (or somebody) but not effect (accomplish) anything seems, then, not to be an exercise of power.’ Finally, Ricken perhaps puts it the most plainly when he says:

> *Intention is essential – if power is causal, it only makes sense if we understand the intention of the person causing the influence of another – if intention is missing, power seems to be the inappropriate term, as coincidental effects of power are neither powerful nor determinable – power is a means for a purpose* (Ricken 2006, p. 544)

The importance of a goal for any exercise of power is consistent across causal, procedural, and productive approaches to power. For causal accounts, which are concerned with how power is used to cause states of affairs to come into being, power only makes sense if it is exercised with the goal of a certain state of affairs in mind. Similarly, in a procedural account, there is no sense in undertaking a “power-procedure” without some goal or desired outcome from that procedure. And again, as Foucault says in his account of power, ‘there is no power that is exercised without a series of aims and objectives.’ (Foucault 1988, p. 95).

When answering the question “what is the intended outcome of power?” it is important to consider what kind of a goal power can be aimed at. Here there are a wide range of possibilities. For Hobbes the goal of power is obtaining “some future apparent good”(Hobbes 2018, p. 76), while both Russell and Goldman frame the aim of power as bringing about some desired effect, thing, or state of affairs (Lukes 1986, pp. 19, 157). For Dahl, Lukes, and Weber (Lukes 1986, pp. 34, 39), the central goal of power is altering or affecting the behaviour of others, by either making another do something they would not normally do or otherwise overriding their interests and changing their behaviour. Parsons (Barnes 1988, p. 58), Morriss, and Galbraith (Clegg 1989, pp. 9, 30) approaches to power allow for both of these kinds of goals. We can see from even a brief look at the literature that what constitutes a goal of a mode of power can be left broadly open but, generally speaking, so long as it is the bringing about of some desired end or effect it is an appropriate goal for power.

It is important to note that in saying that all exercises of power are goal-oriented I am not claiming that power can only be exercised intentionally. Power may have effects that serve a particular goal or purpose, even where those specific effects were not consciously designed or intended. The claim is that there is a kind of purpose to the exercise of power, even where that exercise may be unintentional to some degree. For example, Lukes describes a kind of power where *A* exercises power by shaping the or determining what *B* feels their interests are (Lukes 2005, p. 27). This includes examples where *B* is not aware of the operation of power but can also include situations where even *A* is not aware they are exercising power. A tenant may act in certain ways around their house because of the exercise of power by their landlord, even where that landlord has not intentionally or specifically directed the tenant to behave in certain ways. This is not an intentional exercise of power, but there is still a purpose or goal behind it, namely to induce a tenant to care for the property they are renting.

The following chapter explores, in more detail, four examples of the application of big data as a technology of power, in order to demonstrate the value of this approach. But it is useful here to briefly mention one of these examples to show the kind of goal that may be drawn out through this analysis. The Chinese government has for some years now been trialling a social credit system, whereby citizens receive ratings based on their behaviours indicating their general reliability and trustworthiness (Botsman 2017). Government bodies and corporations in China have been using masses of collected data to algorithmically generate these scores, and those with high scores are rewarded with fast-tracked access to healthcare and the ability to avoid paying deposits on hotel bookings and bike rentals (Huang 2017), while those with low scores have been punished through public humiliation (Raphael & Xi 2019) and restrictions on train and plane travel (You 2018). In this context, when we ask the question “what is the intended outcome of power?” the Chinese government’s stated aims are to ‘…forge a public opinion environment where keeping trust is glorious. It will strengthen sincerity in government affairs, commercial sincerity, social sincerity and the construction of judicial credibility.’ (Botsman 2017). In other words, the goal of power in this context is increasing population compliance with laws, rules and social norms.

Agent

The second question to answer is "who is exercising power?". Here we look to both name the agent(s) behind that particular exercise of power and to identify who, more generally, has access to that kind of power. It is important to clarify the use of the word "agent" here. A pluralistic approach to power holds that there is a wide variety of possible answers to this question, and in some cases, it will be possible to identify a specific agent such as a particular individual or group of individuals. In other cases, it may be more appropriate to identify more abstract "agents", such as inanimate objects or abstract structures, such as algorithms, physical architecture, or social conventions. This is a strength of a pluralistic approach to power, as it allows us to see those contexts where power is exercised by agents and those contexts where power is structural clearly. What the term "agent" here means is the "source" of the force of power, be that an individual, a group, or a broader structure, depending on the features of the context.

Many accounts of power either explicitly or implicitly construct power as a thing that is deployed by some intentional agent. For example, Hobbes describes power as a *man*'s means to obtain a future good, and both Dahl's and Lukes' constructions of power require an agent, *A*, who uses power on another. Machiavelli also presupposes some individual using power within a political arena, as does Weber when he discusses the chief at the head of the bureaucracy. And when Parsons positions power as the means by which an individual directs social action, he constructs power as needing an individual who exercises it. Foucault is perhaps the odd one out in the taxonomy above, in that he constructs power without a single central agent. As power for Foucault exists across multiple points within relationships, there is no central human agent behind power generally, but there is nevertheless a sense in which there is agency to the operation of power as those parties within the relationship interact with and impact on each other, and we can talk about the structures around us as "agents" in a sense in that they can be the source and the moderating influence of power.

It is not necessary that the agent behind power be a literal human agent, or even a group of human agents. It is possible for it to be an abstract, or inanimate agent. A share trading algorithm automatically executing a buy order is an agent in this broad sense. Even where the agent of power is a machine there is an intentionality behind it. Non-human agents are generally subordinate instruments of some human purpose.

Beyond the idea of the agent of any given exercise of power, a mode of power will be generally more or less accessible to different agents. In answering the question of who (or indeed what) is the agent behind a mode of power, it is helpful to also consider more broadly to whom that mode of power may be accessible to, and indeed naming the agent will help us answer this second consideration as well. There are many factors relevant to determining the accessibility of a mode of power. One of these factors is the presence of a relationship. In a mode of power whose access is limited by the presence of a relationship, only those within that relationship will have access to that mode of power. For example, a mode of power that arises from an employer/employee relationship will only be accessible to those within an employer/employee relationship. A second factor is the availability of resources or technical capabilities. Any mode of power that requires the expenditure of time, labour, money, or the use of some resource or specific technology will be restricted according to who has access to those required resources. Instruments of power associated with governments often require considerable resources, such as a standing army or a mass surveillance network, and such instruments are out of reach of those without the requisite resources. A third factor that may influence the accessibility of a mode of power are prevailing customs or ideologies. There may be modes of power that, as a result of tradition or ideology, are associated with certain individuals or classes of individuals, and thus are inaccessible by those without a particular social status. Many economic modes of power are associated with the prevailing economic ideology, so in many countries currently those modes of power will be more accessible by capitalists than by others.

As an example, consider the ways in which the company Amazon is using big data to monitor and control its employees. Again, this case will be explored in more detail in the following chapter, but it is useful to briefly look at this context here regarding the agent of power. Amazon was an early adopter of big data through innovations in the algorithmic recommendation of products to shoppers, but it has also been turning its formidable data collecting and processing capabilities on its employees (Kantor & Streitfeld 2015; Liao 2018). The movements of Amazon's warehouse employees are monitored using GPS trackers and ultrasonic wristbands, and their performance is evaluated by algorithms. Those who perform well are rewarded with bonuses and perks, and those who perform poorly are reprimanded, demoted, and fired. In this context, the agent of power is management, whether that be a direct supervisor or higher levels of management. When a supervisor administers reprimands or gives rewards, that supervisor exercises power as a delegate of the company's executive board.

Subject

Thirdly, we need to answer the question "who is power exercised on?", that is who the subject of a mode of power is. Briefly, the subject of a mode of power is the target of an operation of power, the individual or group that a mode of power takes hold of and acts on in order to pursue its goal. Generally, the subject of a mode of power will in some way be related to the goal of a mode of power. For example, if the goal of a mode of power is to change the behaviour of a person or group, the subject of that mode of power will be those persons, or if the goal of an exercise of power is a more abstract goal such as increased profits, then the subjects will be those people who need to be acted on to achieve that goal such as employees. Of course, there are kinds of power that can be exercised on and over non-human animals and inanimate objects, but I am primarily concerned here with those kinds of power that have people as their subjects.

Just as we can see broad support for the ideas of power as goal oriented and agential in nature, we can see similar support for the idea that power is exercised over a subject or subjects. Many writers explicitly address the idea of the subject of power as part of their construction of power. Dahl, Lukes, Weber, and Parsons construct power as something that affects a subject. Dahl and Lukes both include the subject within their more formulaic definitions of power, while both Weber and Parsons are concerned with how power directs the actions of those who are subject to power. Foucault also explicitly addresses the importance of the subject, though for Foucault power does not simply "act" on a subject. Rather, individuals, including those who may be in positions of power, are subjectified by the operation of power. Even those writers, like Hobbes and Machiavelli, who do not explicitly address the idea of a subject of power still construct power such that it operates on a subject. In describing the different forms of power, Hobbes suggests that power functions on other individuals, as power works to make others respect or fear the agent who is exerting power. Similarly, a Machiavellian strategy of power as the deployment of strategies to influence and "defeat" others requires the assumption that power acts on those others as subjects.

In some ways, this question will be the easiest to answer in the context being examined, but we must take care to properly ask and answer this question in each context. A good example of this is in the context of the use of automated facial recognition technology by law enforcement agencies. Across the world, law enforcement agencies have turned to big data to identify and track individuals within crowds. Chinese police have been using the technology to monitor citizens as part of a program of public shaming of jaywalkers (Ricker 2019), and also to track and round up over one million Uyghurs (a Muslim ethnic minority in the western provinces of China) into forced labour camps (Barbaro 2019). Meanwhile, American police forces have used the technology to track individuals at protests and as a tool in arresting individuals for offences (García-Hodges et al. 2020). When we ask the question "who is power exercised on?" in this context, the answer are those persons of interest to the authorities. While this in some ways a broad answer, it is still determinable in that the details of the context being investigated will allow us to pick out who is a person of interest. For example, in the case of the American police or Chinese authorities tracking jaywalking, the person of interest is a specific, often named, individual, but in the context of the use of facial recognition to track the Uyghur people, the persons of interests are any members of a broader group. Again, I will be exploring this context in more detail in the following chapter.

Means

Finally, we arrive at the fourth question: "how does this power function?", and by asking this question we look to set out the means of a mode of power. By means, I refer to the mechanisms, techniques, and practices by which a mode of power acts on its subjects in pursuit of its goal. For a mechanism, technique, or practice to make up the means of a mode of power what is necessary is that they provide a way in which power can take a hold of its subject. That is, they must be capable of directly or indirectly impacting or affecting the subject of a mode of power. Different mechanisms, techniques, and practices will of course affect subjects in different ways, but what is essential is that they have some effect on the subject of power. Without this, the mode of power would be largely toothless, with no real method by which it can work towards pursuing its goal. In comparison to the first three questions surrounding the goal, agent, and subject of a mode of power, the question "how does this power function" has the widest range of possible answers. As such, this is not an attempt to produce a comprehensive list of the various mechanisms, techniques, and practices that a given mode of power can utilise. What is much more practical is to assess them on a case by case basis. However, it is possible to make some general comments about the kinds of mechanisms, techniques, and practices that make up the means of a mode of power.

We can roughly characterise a mechanism, technique, or practice as either direct or indirect, and active or passive. By direct or indirect, I mean that the mechanism, technique or practice either directly affects the subject of that mode of power or that it indirectly affects them. The difference between a direct and an indirect mechanism is a sense of distance between the mechanism and the subject of that mode of power. A direct mechanism is immediately applied on the subject of power, whereas an indirect mechanism functions at a greater distance, removed from the subject but still influencing them. The use of violence on a subject is a prime example of a direct mechanism. The target of the mechanism is the subject directly, and the mechanism allows the mode of power to directly impact on that subject. A good example of an indirect mechanism however would be surveillance. Even where surveillance is aimed at an individual specifically and based on that surveillance that individual alters their behaviour, the surveillance is operating on that individual in an indirect manner as it acts at a distance from the individual.

Beyond the distinction between direct or indirect, we can also distinguish between active and passive mechanisms, techniques, and practices. Active means of power are those mechanisms, techniques, and procedures which are actively implemented or deployed by those agents exercising power. These would include direct statements and actions from the agent exercising a mode of power, such as the issuing of a threat or command, or the infliction of direct violence or force. It would also include other mechanisms or techniques such as surveillance of the subject or using (or requiring the subject to use) a specific technology or platform. What makes these, and other mechanisms, active is the involvement of a direct action or decision by the agent to take a hold of the subject in some way. Importantly, an active mechanism can affect the subject directly and/or indirectly. A threat affects a subject directly, but the use of surveillance may affect a subject more indirectly, but they are both active mechanisms of a mode of power.

In contrast, passive means are those mechanisms, techniques, and procedures which operate passively in the background and can be picked up or relied on by a mode of power. Passive means might include pre-existing social norms or practices which a mode of power can rely on or encourage as a means to affect a subject, or it may be the physical (and social) architectures around a subject that allows a mode of power to act on them. The operation of a passive mechanism, technique or procedure is generally automatic, and does not rely on the attention or involvement of the agent behind that mode of power. Some passive mechanisms may begin as active but over time become passive. For example, there may be the active decision to design architecture a certain way or encourage the development of a new social norm, but over time those mechanisms become passive as they operate in the background, picked up by a mode of power as they become relevant to its operation.

The answer to the question of "how does this power function?" will often be a list of various techniques and technologies, and this is clearly evident in the fourth example which I will be exploring in the next chapter, where big data is used to track and control the spread of COVID-19. Following a cluster of pneumonia cases in Wuhan, China in late 2019, a novel coronavirus was identified and rapidly spread across Asia and the world (WHO 2020). The World Health

Organization declared COVID-19 a pandemic on 11 March 2020, and governments and health authorities across the globe have turned to big data as part of the effort to contain the spread of the virus. Broadly speaking, big data is being used to model the movements of populations and the virus, to document its spread, and as part of contact tracing efforts to identify who has come into contact with an infected person (Wong 2020). As such, when answering the question of "how does this power function?", there is a list of different techniques and technologies we need to attend to. This list includes the threat of sanctions such as fines or imprisonment, but also includes different forms of surveillance. These surveillance techniques and technologies include bottom up techniques where personal mobile phones are used to track the people someone comes into proximity with and top down approaches where mobile phone GPS data is used to track the movement of populations, while Quick Response (QR) codes and digital sign ins are also used to register who moves where at a given time.

Identifying the Mode of Power

Once we have asked more focused questions, such as those explored above, and set out the key contextual features, we can then use them to identify the relevant conceptual features of different theoretical accounts of power. By conceptual features, I mean those key characteristics or innovations of a theoretical account of power that show how power functions. So for example, a key conceptual feature of Hobbes' account of power is that power is self-reinforcing, in that as it is exerted it tends to put an individual in a better position to exert even more power, while Weberian power requires the presence of expertise, or technical and procedural knowledge, as a key feature, and Foucault's account of power has as a key conceptual feature the presence of constant and overt surveillance. The presence of these conceptual features in the context we are studying, as indicated by the contextual features we have picked out, will show us how power operates within that context. In some cases, we will find contexts that clearly line up with all the conceptual features of one account of power, while in others we will find conceptual features from different accounts, showing us instances where the operation of power does not neatly fit into one single theoretical analysis.

For the purposes of this thesis, I will be drawing from those accounts of power included in the taxonomy above, but this analysis could be extended to other accounts of power not considered here. In doing so, it is important to pick out the central features of that account of power that set out how power operates. These central features may include the processes thorough which power can be exercised, the necessary techniques for a successful exercise of power, the sources of power, or some other crucial element. They will largely relate to the theoretical innovations developed by the theorist behind that account of power, as these innovations will be what sets that writer apart from other theorists of power. For convenience, I will briefly revisit those accounts of power included in the taxonomy above, and briefly list the key conceptual features of these accounts.

Account	Key Features of Power
Hobbes	• Power is exerted rather than exercised • Power is derived from a natural or instrumental source • Power is self-reinforcing, in that the exertion of power places an agent in a better position to exert further power • Power operates against and from a background threat of force
Dahl	• Power exists in a relationship whose parties have conflicting desires • Based on the actions of one party, another party performs or refrains from performing a certain action • Power can be identified through counterfactual reasoning • Power has a base, means, scope, and amount
Lukes	• Power is exercised where one party affects another contrary to their interests and in a non-trivial manner • 1st Dimension: o The features of the first dimension of power are the same as the features of Dahl's account of power • 2nd Dimension: o Parties have conflicting interests, rather than just desires o The actions of one party creates or reinforces social practices that discourage another from raising their own interests o Power can be identified through counterfactual reasoning • 3rd Dimension: o Power works to reinforce the status quo o The exercise of power is accepted as normal or natural o Latent conflict – the subject of an exercise of power adopts the interests of the agent as their own o Power can be identified through counterfactual reasoning
Machiavelli	• Power is comparative, in that a person with more power has a greater scope for action in relation to others • There is the possibility of winning • Power exists in direct competition between parties in two senses: o Exercises of power compete or conflict with each other o The exercise of power is part of the struggle to secure further power
Weber	• Power requires a legitimising source such as the rule of law or legal authority • Power can only be exercised through manipulation of the rules of the system by an expert with both technical and procedural knowledge • The agent and subject of an exercise of power must have a common

	membership in the system
Parsons	• Power is exercised through the securing of the performance of obligations or the control of other’s decisions • Power exists in either primitive systems based on force or complex systems based on legitimised authority • Power is exercised through four strategies based on positive or negative sanctions and the manipulation of situations or symbols: i. Persuasion ii. Inducement iii. Activation of commitments iv. Coercion
Foucault	• Power exists within social relationships where divisions and differences between parties across that relationship define the parties • Power shapes individuals into idealised subjects • Power is diffuse in nature, acting across the whole relationship • Resistance is always possible through the shaping of the relationship “from below” • The exercise of power relies on constant and overt/visible surveillance • Power works through dividing individuals into categories of normal and abnormal

Conclusion

In the current literature, there is a focus on the search for a single, unified theoretical account of power that best explains the relationship between big data and power. Whether that be an updated form of Foucauldian power such as Deleuze’s work on control, or the development of a new kind of power such as metric power or smart power, the general aim in the current debate is to identify the account of power that best explains how big data is used. However, this approach is misguided at best as it generalises the many different phenomena we use the word power to refer to. Just as big data is an umbrella term for a wide range of technologies, so too is power. We cannot then use a generalist account of power to understand how exercises of different kinds of power use different big data technologies across diverse contexts such as governance, advertising, criminal justice, credit reporting, and many more. To do so will miss important details in each context, potentially limiting our ability to create meaningful legal and ethical protections against harm.

We must instead take a pluralistic approach towards the concept of power, where we can use the conceptual tools provided in different theoretical accounts of power to understand the nuanced differences in the operation of power across different contexts. By taking this approach, we can then direct our attention to identifying the particular mode or modes of power operating in the contexts under investigation, by asking more targeted and focused questions at an appropriate level of abstraction. These questions are “what is the intended outcome of power?”, “who is exercising power?". "Who is power exercised on?", and "how does this power function?". This will allow us to pick out in any given context the goal, agent(s), subject(s), and means of power, and in turn will help us understand how power functions within that context as these contextual features will indicate the presence of different conceptual features of various theoretical accounts of power.

This approach is particularly important when we are investigating the relationship between big data and power, because of the many different technologies that make up big data. We cannot adopt a single theoretical understanding of power when we are studying the use of big data, because big data is an umbrella term for such a wide range of different analytical technologies and techniques. In the following chapter, I will demonstrate the value of this approach by applying it to four example contexts where big data is used as a technology of power. By using this approach, we can see that in some contexts big data is used as part of an exercise of a mode of power that clearly aligns with one theoretical understanding of power, while in other contexts we can see different kinds of power working alongside or potentially even overlapping each other. This is important, because it allows us to address the operation of power and the use of big data in each context specifically and develop more effective protections based on the operation of power in that context.

Chapter 4

Modes in Practice

In the previous chapter, I proposed that we take a pluralistic attitude towards power which allows us to identify the mode(s) of power within a given context by setting out the conceptual features of theoretical accounts of power and the contextual features of the phenomenon we wish to examine. In this chapter, I demonstrate the value of this approach by examining four contexts in which big data technologies are used as an instrument of power. In these contexts, this approach can help us identify key details about the operation of power in the digital age and how big data is used as part of decision-making processes. It can also help explain how the use of a new technology changes the operation of power, which is the primary focus of the next chapter. The aim of this chapter is to illustrate the importance of attending to the specific forms of power operating in each context, and the kind of data analytics employed to amplify that power.

The first set of examples are the social credit systems currently in operation across China. Vast amounts of data are being collected about the activities of Chinese citizens, and this data is being collated into social credit scores, ranking individuals as consumers and as citizens. These scores are then being used to inform decision-making processes, ranging from finance and loan approvals to denying individuals access to travel or higher quality health services. In this context, we can see the key elements of Foucauldian disciplinary power, where citizens are being trained by constant, overt surveillance to conform to social norms as citizens and consumers.

In the second example, we will look at how companies such as Amazon use big data to monitor employees, as well as goods and materials in the workplace. Amazon is at the forefront of the use of big data to track the physical products it sells and ships, as well as the employees who both handle that product and work in Amazon's offices. Workers in Amazon's warehouses wear GPS trackers and wristbands that use haptic and audio feedback to both guide and track their movements, while those who work in office positions have their work constantly monitored and compared against the work of colleagues on a range of performance metrics. Those employees who fail to meet productivity targets in the warehouse or the office may be reprimanded or fired, while those who do well are rewarded with bonuses and prizes. In the case of Amazon, we can identify characteristics of both Foucault's productive account and Parsons' procedural account of power, as management look to directly control the actions of employees through techniques of subjectification.

This chapter then examines the use of automated facial recognition technologies in law enforcement. Increasingly, police departments and other law enforcement agencies across the world are turning to facial recognition to control crowds, monitor protests, track and identify criminals and suspects, and in extreme cases, to target state-sanctioned violence. The identification of individuals through automated facial recognition is being used as the basis for a range of decision-making processes by law enforcement, including the critical decisions of who is monitored and who is detained by the state. In the use of facial recognition, we can see the features of Dahl's causal account of power, as the technology is playing a central role in causing individuals or groups to act in ways they would otherwise not act.

Finally, the fourth example is the use of various big data techniques in response to the threat posed by the COVID-19 pandemic. Following the outbreak of the COVID-19 pandemic in the first half of 2020, governments and health authorities across the world have turned to big data for tools to track and manage the spread of the virus. These uses include tracking the movements of populations through mobile phone geolocation and internet browsing data, tracing who comes into contact with infected individuals, and using camera-based surveillance to monitor social distancing requirements. These collected data are being used by governments to inform decision making around restrictions on public and economic activity, as well as to enforce these restrictions. Importantly, in this context we see features from three different accounts of power, namely Parsons', Foucault's, and Hobbes' accounts, overlapping with each other and working in parallel to create a detailed and nuanced web of interrelated kinds of power.

Social Credit

While Western countries have an extensive history with financial credit systems, it is still a fledgling industry in China. Until the 1990's credit was rarely used across China, as households tended to rely on savings rather than loans or credit cards. As late as 2015, Chinese households saved 36.1% of their income, compared with Australia and the US where households saved 8.9% or 4.9% of their income respectively (Sun 2020). In 2003, the Central Committee of the Chinese Communist Party first proposed the idea of a social credit system, though at the time it was unclear if they were simply referring to a socialised version of an otherwise capitalist system (Chorzempa et al. 2018, p. 3). Over the next few years, financial companies began developing credit score systems, until June of 2014 when the State Council of China released a policy paper titled 'Planning Outline for the Construction of a Social Credit System' (Botsman 2017).

This paper outlined a dramatically expanded vision for the credit system and introduced the idea of 'social credit', essentially a trustworthiness or sincerity score awarded to an individual or business intended to

> *…forge a public opinion environment where keeping trust is glorious. It will strengthen sincerity in government affairs, commercial sincerity, social sincerity and the construction of judicial credibility.* (Botsman, 2017)

The social credit system has two main elements: a huge interconnected database, linking data held across a wide range of government and non-government bodies across China about individuals and legal entities such as businesses and government departments, and a system of rewards and punishments to encourage individuals to be more trustworthy (Chorzempa et al. 2018, p. 2). The general aim of the Chinese government is to establish, if not a single centralised system, at least the framework through which several social credit systems will function across the country.

Currently, there are a mix of state and non-state social credit systems in China. Those run by non-state organisations function as a kind of rewards system, while those attached to the state have access to a wider range of punitive functions. Amongst the non-state systems, the largest is

Zhima Credit (also known as Sesame Credit), with over 520 million users in 2017 (Koetse 2018). Zhima Credit is developed and run by Ant Financial Services Group, who is also the developer of AliPay, the most used payment system in China, and an affiliate of the largest e-commerce site in the world, Alibaba. As a result, Ant Financial has access to data on the online habits of hundreds of millions of Chinese nationals. This dataset is then augmented with data drawn from public databases, such as those run by China's Public Security Ministry and State Administration of Taxation, and other large private databases including from Didi Chuxing, a major ride-hailing service, and Baihe, the largest Chinese dating website (Botsman 2017).

A Zhima Credit score ranges between 350 and 950 points, determined by a proprietary algorithm. While the full workings of the algorithm have been kept secret by Ant Financial, "consumers" are advised that the data used to determine the score are drawn from five categories (Banking 2016). The categories, and their approximate weightings, in the algorithms are:

- **Credit History (35%)** – a user's payment and debt history. This category includes things like credit card repayments, utility bill payments, ratings on e-commerce sites like Taobao (similar to eBay), and other similar information. This category is closest to what credit ratings in Western countries have typically been based on as well.
- **Fulfillment Capacity (20%)** – a fairly nebulous category generally reflecting the user's ability to fulfil contracts and other obligations. Evaluated based on information about major assets such as property and car ownerships, payments towards insurance policies, as well as how much each user also uses Alibaba's other financial products and their Alipay account balance.
- **Behaviour and Preference (20%)** – the online behaviour of consumers, including data like rate of activity, websites visited, product categories purchased, and consumer segments the user belongs to. An example is the difference between someone who purchases diapers and someone who plays online video games. An individual who regularly purchase diapers is likely a parent and is apparently responsible, while someone who spends ten hours a day playing online video games would be rated down for being idle (Xu & Xiao 2018).
- **Identity Characteristics (15%)** – the user's personal information, including things like home address and length of time in that home, phone numbers, education level, employment, and official information like licenses. Users can also link information from other accounts and services like LinkedIn. While users are not currently required to provide this information to the Sesame Credit system, entering personal information rewards an easily obtainable boost in score.
- **Social Relationships (5%)** – tracks the user's interactions on social media to see who and what influences the user, who and what they influence in return, and the scores of those that the user regularly connects with.

A user's score functions as the basis for various decision-making processes. For example, users with a score of 588 receive a five day free membership to Baihe, a score of 669 allows them to waive deposits when booking select hotels or bike rentals (Huang 2017), while a score of 770 also allows for waiving deposits on some home rental applications, as well as improved access to healthcare and prestigious schools (Carney 2018). Zhima Credit is not the only non-state social credit system in operation. Tencent Holdings Ltd. recently released a competing platform using data from its WeChat app, one of the largest multi-purpose social media, messaging, and payment apps in China (Yue & Yingzhe 2020). Initially, the Chinese government issued licenses to companies including Ant Financial to develop official nation-wide systems, which would be run by those companies on behalf of the government. However, these licenses have not been renewed, and the result is that a hybrid of state and non-state social credit systems has developed in China.

The various state-run social credit systems in China can be broadly grouped into three categories. The first are local or city-based systems. These systems apply to the residents of a certain local government area or municipality. The city of Rongcheng, for example, has developed a social credit system where citizens start with default allocation of 1,000 points (an A rating). Gaining points can increase that rating to A+ while losing points can lower a person’s rating to D (Raphael & Xi 2019). Citizens across the 919 villages that fall under the jurisdiction of Rongcheng can earn points by pruning their neighbours trees (1 point), taking an older neighbour or relative to the hospital (1 point), helping to read a water meter (0.5 point), or visiting an elderly neighbour to cook and clean for them (4 points), amongst other activities. They can also be fined and lose points for things like letting chickens escape a coop (200 yuan fine and 10 points), dumping waste in a river (500 yuan and 5 points), getting into a fight (1,000 yuan and 10 points), or graffitiing or posting messages critical of the government (1,000 yuan and 50 points). As citizens’ ratings fall, they suffer increasingly severe punishments. Falling just one point below an A rating (a B rating on 999 points) renders a citizen ineligible for a mortgage. Falling to an even lower score results in restrictions on hotel room bookings, access to high-speed rail travel, and on participation of one’s children in extra-curricular activities. Ratings also apply to companies, and those with lower scores are ineligible to submit tenders for local and state government contracts (Raphael & Xi 2019). Additionally, activities that result in lost points that are captured by security cameras are broadcast on radio and TV, and the perpetrators are identified by name. One nightly TV show in Rongcheng called *People’s Live 360* shows surveillance footage of jaywalkers, speeding drivers, and washing being hung on balconies, alongside the faces and names of those whose actions have lost them points.

Some cities, such as Hangzhou operate a second kind of social credit system, a hybrid one, where a government system is combined with a private one (Raphael & Xi 2019). In the case of Hangzhou, the municipal government has joined forces with Zhima Credit. Initially, in 2004, Hangzhou issued magnetic strip cards to residents serving as a social-security card, transport card, a means to pay traffic fines, and to access parks. The data from these cards was then recently combined with the database of those residents who also have a Zhima Credit score. Those who combine their scores have them linked through facial recognition tools, and the government can use the Zhima score to gauge the trustworthiness of citizens while Ant Financial gains access to the taxation and other government-held data of those users. Unlike Rongcheng, where drops in score lead to increasingly harsh restrictions on individuals, the system in Hangzhou still operates more like a loyalty reward program, where higher scores entitle individuals to extra benefits and advantages.

Finally, the third kind of social credit systems are those that operate across municipalities or, in some cases, across the entirety of China. One such system has been attached to the court system in China. Those individuals, companies, and (occasionally) government agencies who do not comply with a judgement handed down by the court can now be added to a judgement blacklist system (Chorzempa et al. 2018, p. 4). In a way, this system is a practical punishment for contempt of court. Those who find themselves on the blacklist are publicly listed on an online platform, and as the blacklist is integrated with databases from securities regulators, the central bank, and the company registry, individuals on that list are blocked from issuing securities or borrowing money. Further, individuals can find themselves unable to book air tickets or high-speed rail tickets. As of May 2018, some 11.14 million citizens have been blacklisted from buying flight tickets, and 4.25 million have been blacklisted from buying high-speed train tickets (You 2018).

Across these various systems, the initial plans appear to have been for a grand unification, whereby the private databases of those running non-state social credit systems are combined with government databases to create a comprehensive system running across the entire state. This appears to be at least delayed if not partly abandoned as local government bodies develop their own patchwork of systems and non-state ones have not been issued licenses to run an official program nation-wide, but over time databases continue to be linked, and the network of social credit systems becomes ever more pervasive.

Power in the Social Credit System

Looking at how the Chinese social credit systems function through the theoretical lens of different modes of power, we can ask the question “who is doing what to whom for what outcome?” and identify the goal, agent, subject, and means of power that operates through the social credit system, which will then help us to align this context with a theory of power. Firstly, what is the intended outcome of power here? We can turn to the stated aims of the Chinese government as set out in the Planning Outline mentioned above for guidance here. According to the Chinese government, the official purpose of the social credit system is to foster trust in public institutions such as courts and in business dealings (Botsman 2017). But we must also look at how the system functions to understand the purpose of power in this context. We can identify the goal in this context from the categories of behaviour that are penalised, such as jaywalking, disturbing the peace, fraud, failure to pay fines, and criticising the government. Clearly the social credit system is aimed at not just building public trust, but also in suppressing antisocial behaviour, criminal activities, and political dissent. As such, we can say that the goal of power in this context is the normalisation of the citizens and companies of China such that they are more productive, docile, and compliant.

Secondly, who (or what) is the agent behind power here? There are a few agents at play in this mode of power. The most important agent is the Chinese government (both at local and national levels of government), but there are also many private companies such as Ant Financial and Tencent. Importantly, this mode of power is accessible to anyone who can run such a social credit system, which is primarily dictated by both access to a large enough database to run the system, as well as permission from the Chinese government to do so. Thirdly, the subjects of this mode of power are those individual citizens, companies, and agencies who either live or operate within a specific jurisdictional area or sign up for inclusion in the system voluntarily. Potentially the entire Chinese population, as well as all Chinese businesses and institutions, are eligible subjects of power in this context. Importantly, all these subjects are also ultimately people. The individual citizens who are subject to this mode of power are obviously people, but in targeting companies or corporations, the system is still ultimately targeting the behaviour of the people who make up those companies or corporations.

Finally, as to the means of this mode of power, ultimately the functionality of the social credit system consists of straightforward rewards and punishments for performing or failing to perform certain behaviours, as well as controlling the assembly and movement of people in time and space. Essentially, the social credit system is a kind of elaborate training system. Those who behave in ways that are deemed trustworthy, productive, or otherwise "correct" by those who set the parameters of the system are rewarded, while those who do not are punished, encouraging individuals to behave in accordance with the system. The social credit system also relies on constant and overt surveillance for its functionality, and this surveillance is an important part of the means of this mode of power. Those who are made subject to this mode of power are under constant surveillance, both on- and off-line. Importantly, this surveillance is not hidden or covert. It is made obvious to those being surveilled. Individuals who fall foul of the system are listed publicly on various websites and may even have their names broadcast in public squares and on television. The system is designed in such a way that those who are subject to it are always watched and are made aware that they are always watched.

From these contextual features, we can see many of the conceptual features of a Foucauldian understanding of power. One of the central features of Foucauldian power is that power is ultimately a productive force. The exercise of power, while it may involve repressive force or punishments, works to mould or train people into 'better' subjects of power. This is clearly visible in the context of the Chinese social credit system, as it aims to form normal, productive bodies, formed to suit the needs of the institution they inhabit as well as society at large. The way in which the scores are generated and displayed ensure that those within the system self-regulate and train themselves to be better subjects of power, by becoming more normalised and productive within Chinese society. Though the system may at times involve punitive and repressive measures, such as the denial of travel or loans, the exercise of power through this system is not aimed solely at these measures. It is aimed at shaping people over time, which is one of the central features of Foucauldian power.

Another main feature of Foucauldian power is the divides and differences across social relationships. It is these divides and differences which define the members of that relationship, provide the space for power to operate within the relationship, and shape how power is exercised and felt by those members of that relationship. We can again see clearly the importance of these divides and differences in this context. There are many different social credit systems in operation, and each one is a kind of social relationship between the agency determining the score and those being scored. The differences and divides in those relationships then define the parties and the operation of power. For those systems run by state bodies, the subjects of power are defined as citizens while the agents are defined as government officials or agencies. The exercise of power is then shaped in those systems by that relationship, determining the kind of subjects that the citizens are being trained to be and the punitive measures available to the agent of power. Likewise, in the systems run by private companies, the subjects are defined as customers or consumers and the agents as corporations or service providers, which in turn shapes the operation of power.

Thirdly, one of the central features of Foucauldian power is that it is not exercised from a single central point but is more capillary in nature as it works across all points of a relationship. In the case of the social credit system, while those companies and government bodies administering these systems can be identified as the agents of power here, the power they are exercising is a capillary one just as in Foucauldian power. It is diffused throughout the social credit system, through the many systems that collect data about individuals, the algorithms that analyse this data and create a score, and the rewards or punishments that are promised or threatened based on an individual's score. The most centralised point is the score itself, but even this is not a truly centralised point of power, as an individual may have multiple scores with different companies or government bodies, and the same score may be treated differently by different agencies.

Finally, one of the defining characteristics of Foucauldian power is its reliance on visible or overt surveillance. Power functions to mould individuals through encouraging them to learn to self-regulate or normalise their behaviour, and one of the primary mechanisms for that is the presence of overt surveillance. This surveillance is one of the main characteristics of the social credit system. Those who receive scores may not be locked up in a physical panopticon, but they are being subject to a constant surveillant gaze that captures most, if not all, of their actions. This surveillance is not covert, it is incredibly obvious and deliberately overt, as scores are made visible to individuals as well as suggestions on how they can improve their score, and those who fail to self-regulate may find their names and faces broadcast through the media to shame them into better self-regulation. They are made aware of their surveillance, and constantly reminded of it.

We can clearly see the central features of Foucauldian power in the context of the Chinese social credit system. Power here is working to train the subjects of power to be compliant and normalised citizens and consumers. It also operates as a capillary force, across the network of technologies embedded in the social relationship and the overt surveillance that helps track the subjects of power as well as remind them of their training.

Workplace Management

As businesses and government departments utilise big data to track and understand consumers and citizens, they are also increasingly turning their gaze inwards and are using big data analytics to monitor and analyse their employees. As a result, big data is altering the nature of the relationship between employer and employee, and the power present in that relationship. Performance analysis can extend beyond current employees to potential employees and ex-employees. For example, many companies are using big data analytics as part of their hiring procedures (Barocas & Selbst 2014; O'Neil 2016, p. 105). Employers have long used personality assessments as part of later stages of hiring processes, but prospective employees are answering more data driven assessments early in the application process, sometimes at the point of the initial job application. Applications are then whittled down by these data driven processes before they progress to review by a human decision maker. However, our concern here is with the use of big data to monitor employee performance at work.

Dell is one company that has employed big data techniques to manage the performance of employees in order to place them in the right positions. Sales data like time to proficiency, revenue, retention, and margin attainment is correlated with psychometric profiles in an attempt to identify employees best suited for promotion to positions of leadership in sales (HRD 2018). The United Parcel Service (UPS) utilises sensors in their fleet of delivery vehicles, gathering data about everything, from whether the driver is wearing a seatbelt to how many times the car reverses or must make a U-turn (Marr 2018). UPS says that the data is not used to discipline or even track the drivers themselves, rather to ensure their safety and provide feedback to inform ongoing employee training (Miller 2018), and the results of their data collection are astounding. By 2018, UPS announced that their data analytics have saved them upwards of 8.5 million gallons of fuel and 85 million miles of travel per year and increased the average number of stops each driver makes from below 100 to 120 (Marr 2018). Companies like Humanyze offer wearable technology that monitors employee’s conversations, including the length, tone, and number of interruptions to evaluate employees (Marr 2018). Three Square Market, a technology company that provides self-service mini markets and vending machines to hospitals, hotels, and offices, started experimenting in 2017 with embedding subcutaneous microchips in the hands of about 80 of the company’s 250 employees (Metz 2018). As of early 2019 these RFID enabled microchips primarily act as a form of key-card for doors and computers in the office, as well as a payment method for in office vending machines, but also contain some personal information for identification purposes, and enable the tracking of employee movement and behaviour at work.

There are of course many more workplaces utilising big data driven workplace management technologies, but Amazon is leading the charge when it comes to using big data to manage employees. While there has been a lot of focus in the media around how Amazon uses big data to track consumer behaviour, there is growing interest and concern with how Amazon s uses big data to track and manage its employees. By mid-2020, Amazon had over 935,000 employees worldwide (Nickelsburg 2020), largely divided into warehouse and office staff, each being subject to different kinds of big data driven workplace management. In Amazon’s warehouses, called fulfilment centres, the technology giant uses sophisticated data driven technologies to track and monitor the billions of products it sells every year, and the hundreds of thousands of human employees known as “pickers”. As product enters these warehouses, some of which are as large as multiple football fields, they are stored at random in yellow, tiered bins, and their location is logged and tracked by a computer. When an order is placed for a product, robots guided by barcodes printed on the floor and precise GPS technology navigate to the nearest pod containing that item and carry it to a human picker. These pickers are in turn likewise guided by wearable GPS trackers to the relevant robots and the pods they are carrying (Turner 2016). Workers report avoiding using toilets, instead relieving themselves using plastic bottles, as they fear that the long walk to the restrooms may suggest that they are idling (Liao 2018). Those who spend too much time idling, as indicated by the trackers, fear reprimands or even losing their job entirely.

In 2018 Amazon patented a wristband to track the precise location of employee's hands in relation to stock (Solon 2018). By using ultrasonic sound pulses and radio transmissions, the wristbands provide constant data on the precise locations of employee's hands to supervisors. These wristbands also vibrate and emit audio feedback to employees to guide them to specific stock. Officially these wristbands would function as an efficient way to find stock in a large and crowded warehouse, but they also offer a new level of surveillance and control over employee movements. Warehouse employees are already expected to process hundreds of items in an hour, spending no more than a few seconds on each item. Ex-employees have expressed concern that the data from these wristbands could be used to monitor and punish those employees who do not move fast enough or have their hands 'in the wrong place at the wrong time' (Yeginsu 2018). Such concerns are not unfounded, as in extreme cases, consistently failing to keep up can result in reprimands including the outright termination of employment (Tangermann 2019). Aside from avoiding reprimands or even losing employment altogether, there are also incentives for performing consistently well, such as "swag bucks" (Hamilton & Cain 2019). Swag bucks are a kind of internal currency, awarded to employees who meet or exceed productivity goals. Swag bucks can be used to purchase a variety of perks for employees, ranging from meals from the warehouse cafeteria, t-shirts, water bottles, televisions, Xbox consoles, or even extra work breaks.

While Amazon's office-based employees may not need to contend with GPS trackers or wristband mounted sensors, they are still subjected to big data driven surveillance and analysis. The full details of the systems Amazon uses are kept secret, but a report in 2015 outlined some important details, confirming that Amazon runs continual performance improvement algorithms on its staff (Kantor & Streitfeld 2015). From the moment an employee begins working at Amazon, and in many cases from when they apply for the position, the algorithms track and rate their performance on a dizzying array of metrics. The data that Amazon collects from its customers are linked back to the employees who build the platform those customers use. Data is collected a huge range of metrics, including how much time a customer spends on the site, what they buy, or what they decide not to buy, at what point they "abandon" a book on their kindle, what they stream in relation to what the system recommends they stream and how long a website takes to load. All these data are fed back into an algorithm that rates the performance of those employees involved in designing these systems. The results from the algorithm are used in regular performance reviews and falling foul of these metrics may result in that employee being demoted or fired from the company. Despite these fears, some employees report that within their performance reviews, after being presented with all the ways in which they have failed their performance metrics they are then promoted, leading to them feeling permanently off balance but still grateful to be around, prompting them to try even harder to 'beat the metrics' (Kantor & Streitfeld 2015).

It is not just data from customers that is fed into the performance algorithms, as fellow employees can also submit data to be considered. Using the Anytime Feedback Tool, employees can submit praise or criticism about colleagues at any time (Kantor & Streitfeld 2015). Managers and supervisors see who submits remarks, but those who are the subject of praise or criticism do not typically find out that information. These remarks are combined with other data, and ultimately employees are ranked according to the collected data. It is ultimately in the best interests of employees to do well on these rankings, as the lowest performers annually are removed from projects or from the company entirely. Meanwhile, those who perform well are rewarded with bonuses and promotions and those who are consistently successful can sometimes collect an entire extra salary worth of bonuses by the end of the year.

Power in Workplace Management

The goal of power in the context of workplace management is, primarily, to maximise profits. Profit maximisation requires extracting the maximum productive work from employees while reducing costs wherever possible. More specifically, the operation of power in this context will be an increase of control over the activities of employees, both in terms of direct control over their actions and indirect control through the reduction of resistance. It is through this increased control that the employees will become more productive and/or cheaper for the workplace, thus leading to an increase in profits. The agent of power here is management, whether that be a direct human supervisor or a more abstract agent in the form of the upper layers of a company. While access to this mode of power is broadly restricted to employers, the relative size of the organisation and how the technology is implemented will further determine whether the agent in that situation is an individual supervisor or the company more abstractly. In a smaller organisation or branch of an organisation, or where a supervisor directly implements a workplace management program, it is more likely that the agent will be an individual person. In a large organisation or where the program implemented is imposed from above an employee's direct supervisor, it is more likely that the upper layers of the company are the agent. The subjects on the other hand are much easier to determine. They are the employees who are participating in and interacting with the technology.

As this kind of workplace management technology can take many forms, there are similarly many different means for this mode of power. However, there are some central means that can be identified. The first is surveillance. For this form of power to operate in the workplace, there must be constant or near-constant surveillance of employees. After all, in order to manage and control how an employee works, it is necessary to monitor that employee and know what he or she is doing. Another common technique is the encouragement of competition by means of the 'gamification' of the workplace. Gamification, where elements and techniques of video game design such as rewards are used in non-game contexts like the workplace (Kim & Werbach 2016), is an increasingly commonly used technique to improve employee engagement. Many workplace management technologies that utilise big data rely on gamification or increased competition in the workplace to engage employees (Dimick 2016; Eagleton 2019). Gamification does not just increase employee engagement; it also encourages employees over time to act and work in ways that are approved by the agent behind the operation of power.

Another important technique that this mode of power relies upon is the limiting of options and possibilities, as well as offering incentives and rewards. Compliance with these workplace management programs, both in terms of active participation and then behaving “correctly” within that program, will often result in rewards, while failure to comply will result in sanctions and punishments. An example can be found in the algorithms used at Amazon to monitor and rate employee performance. Those who perform well in the metrics are rewarded with bonuses and increased chances at promotions, while those who consistently underperform have their opportunities restricted or their employment terminated.

While the Chinese social credit system is a clear example of a context which aligns with one theoretical account of power, in this context we can see the features of two theoretical accounts of power. First, the fact that power here is working in a productive manner and the presence of constant and overt surveillance aligns with a Foucauldian conception of power. The employees of Amazon are conditioned over time to be better subjects of power, more ideal employees who submit themselves to the operation of power within the workplace. This is especially true of Amazon office workers who participate in workplace rankings and competitions. There is also the presence of constant, and overt, surveillance, as employees’ every communication, movement, and even thoughts are captured and tracked. These employees are then acutely aware of this surveillance, including promised rewards and threatened punishments linked to the collection of data.

Also present are key features of a Parsonian understanding of power. Firstly, the agent is exercising power to secure the performance of obligations from the subject by influencing or even directly controlling the decisions made by the subject. In the context of Amazon’s workplace management technologies and techniques, we can clearly see direct control over the decisions made by Amazon’s employees as the subjects of power, particularly regarding pickers, the employees who work in warehouses. The GPS tracking devices and wristbands that provide audio and haptic feedback are not working to normalise the workers, they are directing the workers to act in ways that integrate their bodies into the production line. Workers lose autonomy over even small decisions as to how to complete a task and, instead, a pattern of physical motions is directed via their wristbands and tracking devices.

There is an interesting interplay here of Foucault’s and Parsons’ accounts of power. One of the key features of Foucault’s account of power is that it is productive in nature, in that those who are subjected to power are shaped over time to be ideal subjects. Foucault sees this as happening primarily through the force of discipline, where subjects of power self-regulate and train themselves to be idealised subjects. However, in this context we see clearly a feature of Parsons’ account of power, where direct control is exercised over the decision making made by subjects of power. It is this direct control over decision making that is training people to be ideal subjects of power. As people have their decisions controlled and made for them, they are encouraged to continue to act as ideal subjects of power, shaped in the sense of Foucault’s understanding of power through the direct control of decision making that is characteristic of Parsons’ account of power.

Within this context, we can also identify the presence of a kind of complex Parsonian system of power. In more primitive systems of power, the exercise of power is tied to the threat of physical force, but in this context, power relies on a structure of authority that legitimises its use within that system. In this context, the structure is in part made up of the employment contract between employer and employee, which sets out the rights and responsibilities of each party, but more broadly that structure is made up of the complex legal rules and social norms around work. Within the context of the workplace, there is a legitimisation of an employer's power over their employees through the agreement they enter. This legitimisation gives the employer the right to make certain decisions that take precedence over the decisions of the employee, and to manage and control their opportunities and activities within the workplace. Outside the workplace, the power of the employer is not legitimised, and as such they cannot exercise the same right to control the decisions of their employees.

Finally, we can also clearly see the four strategies of power that Parsons identifies within these systems of workplace management (Parsons 1986, p. 104). The sensors, trackers, and data collectors that work to surveil and measure the performance of employees are also being used as part of the four strategies of Parsonian power to control the actions of employees. There is inducement, a positive situational strategy, whereby the situation of the employee is modified using GPS trackers and rewards offered in the form of swag bucks. There is also persuasion, a positive intentional strategy, where the intentions of the employees are worked on in conjunction with the offering of rewards, such as through the use of metric systems that work to convince an employee that doing what their employer wants is in their best interest as well. There is also coercion, a negative situational strategy, and the activation of commitments, a negative intentional strategy, in these workplace management technologies. Employers are altering the situations around employees and the intentions of employees through metrics and surveillance while threatening negative sanctions to ensure compliance.

In the context of Amazon's workplace management technologies, we can see the overlapping of key features of two theoretical accounts of power, namely Foucault's productive power and Parsons' procedural power. Power is working to shape individuals into idealised subjects, not through self-regulation but through the direct control of decision making. It is also relying on constant and overt surveillance, and the legitimising structure of the workplace. Furthermore, we can see the use of all four of the strategies of Parsonian power, namely inducement, persuasion, coercion, and the activation of commitments, to control employees' decisions and actions.

Facial Recognition and the Police

The use of automated facial recognition technology, or AFRT, has become a major topic of concern recently, especially when it is used by police or other law enforcement bodies. There are several uses for AFRT (Brey 2004). It can be used to track a person's face in real-time on a video feed and it can be used for facial recognition, where a face is compared with others in a database in order to find a match. There are two main kinds of face recognition,

1. One-to-one matching (aka verification or authentication) – the system is presented with a face or an image of a face and it is asked to check if that face matches the database. This kind of facial recognition is commonly used as a security feature on modern phones

and computers.

2. One-to-many searching (aka identification) – the system is presented with a face or an image of a face and it searches through a large database for matches, presenting any match above a certain threshold. This kind of facial recognition is commonly used as part of surveillance.

Facial matching is performed by algorithmically mapping the face using one or more of a number of methods, such as by layering multiple photos of the same face to create a map of the different possible variations of that face (Lee-Morrison 2018), or by using a local feature analysis to identify a number of key facial features such as bone structure or skin blemishes (Brey 2004). As an algorithm maps more and more faces, it is trained over time to map faces so they can be found or tracked in a photo or video, and it can then find that person in other photos even where the lighting or angle differs.

AFRT is being used by private companies and individuals, but it is its use by police forces across the globe that is drawing the most attention. China is the world leader in the use of AFRT, with some estimates suggesting that there are over 350 million CCTV cameras in operation in China currently, and a predicted 560 million by 2021 (Ricker 2019). Most of these cameras have AFRT functionality, and one common use is to identify and publicly shame jaywalkers, often by displaying live footage of them crossing the road with their name on screens adjacent to that intersection. However, the most pervasive use of AFRT is in the western province of Xinjiang (Barbaro 2019). Xinjiang, a large region made up mostly of desert and steep mountains, is home to the Uyghur, an Islamic ethnic group. Since the mid-20th century, the Chinese government sought to exercise greater control over the region, and as such encouraged the migration of ethnic Han (the majority ethnic group in China) to the region. Tensions erupted in 2009 following a series of riots in which 200 Han Chinese were killed, prompting a major security crackdown by Chinese police forces in the region.

As part of the crackdown, an extensive network of AFRT capable cameras have been installed across the region, creating what one journalist described as a bizarre contrast between the timeless architecture and modern surveillance technologies,

> *with these tremendously powerful facial recognition cameras hanging from a mud-brick wall … you have this very bizarre contrast of a place that in some ways feels like it could be timeless and 1,000 years old, with these hyper-modern technological solutions attempting to understand and track the populations.* (Barbaro 2019)

These cameras are arranged to track and monitor the movements of the Uyghur population to both prevent the outbreak of any future violence, but also to pressure the community over time into adopting the culture of the dominant Han ethnicity. Even mosques in the region have had cameras installed on their walls to monitor attendees. In 2016, residents in the region were called in for "compulsory medical check-ups" but no health advice was ever given. Instead, authorities collected a range of biometric information including face and iris scans, and blood and voice samples, from individuals across the region, creating a huge database to augment their AFRT capabilities. In addition to this database, it appears that the Chinese government and police forces have accessed other databases, including Microsoft's public access MS Celeb database (Song

2019).[4] As a result of this pervasive surveillance, upwards of one million Uyghur's have since been relocated into "re-training camps" where they are forcefully indoctrinated with Chinese government propaganda and used as a labour force under conditions that arguably amount to slavery. Those who have not been forced into these labour/re-education facilities find that movement outside of the Xinjiang region is essentially impossible and movement within that region is strictly controlled and regulated through AFRT surveillance.

Of course, AFRT is commonly used in other countries as well. Police in London have been using AFRT from as early as 1998, and in the US police trialled the technology in Florida in 2001 (Mann & Smith 2017, p. 124). Over the following two decades AFRT spread across these two countries, and others, and in 2016 one study found that one in four state or local police departments in the US had access to AFRT, as well as many federal agencies (Horowitz 2020). As the technology has grown more common, different government agencies have begun sharing data to build up AFRT capabilities. Australia announced the National Facial Biometric Matching Capability in 2015 to allow all federal and state agencies to share facial templates (Mann & Smith 2017, p. 127), and the photos in drivers licences are often included, meaning that nearly half of all Australian adults have their faces stored in police operated AFRT databases (Horowitz 2020).

The full extent of how police forces in the US, UK, Australia, and other countries, use AFRT remains unknown, but in early 2020 journalists from the *New York Times* published an exposé of the relationship between US police forces and Clearview AI (Hill 2020). Clearview AI, a technology company founded by Australian entrepreneur Hoan Ton-That, developed facial recognition software that identifies individuals from photographs by matching against a database of more than 3 billion images. Clearview AI controversially obtained most of these photos by scraping "public" images from millions of websites, including major platforms such as Facebook, YouTube, Twitter, Venmo, and Instagram. At the time of the exposé, Clearview AI was providing services to over 600 law enforcement agencies across the US (Hill 2020), to federal and state police in Australia, and several police departments in the UK and Canada, although it has since ceased trading in Canada in response to local investigations (Hamilton 2020). Law enforcement officers who have used Clearview AI's services say they have used AFRT to help in solving a wide range of cases including shoplifting, identity theft, child exploitation, and murder.

Minority community members, particularly members of racial minorities, are particularly concerned about the use of AFRT by law enforcement agencies. There is growing evidence that currently available AFRT systems misidentify African American and Asian faces between 10 and 100 times more frequently than Caucasian faces, with the error rate only increasing for female faces (Singer & Metz 2019). Members of these communities are concerned that an incorrectly identified face can result in consequences for individuals ranging from missing flights, lengthy interrogations, or false arrests. We can already see that such concerns are well founded. For instance, in June 2020 Robert Williams, an African American man, was wrongly arrested on the basis of AFRT identification for a 2018 shoplifting offence that he did not commit (García-Hodges et al. 2020). In

[4] The MS Celeb database was shut down in June 2019, but before it closed it was the largest publicly accessible facial recognition database with over 10 million images from over 100,000 individuals.

response, major technology companies IBM, Amazon, and Microsoft announced that they would stop providing AFRT to police departments either permanently or until clearer regulations are put in place, while some major cities like San Francisco and Boston have banned the use of AFRT locally (Horowitz 2020). Despite this, there are still several vendors continuing to offer AFRT to police units, including Clearview AI.

Power in Facial Recognition

In the context of the use of AFRT by the police, the goal of power is to control or direct the actions of persons of interest. If a person is identified at an airport as someone who is not allowed to cross the border, then they will have their movement stopped by authorities, who will then control their movements. If an individual has a warrant out for their arrest, and AFRT detects them in a crowd, the police can then use that identification to move in and control the actions of that individual by taking them into custody. The purpose of power is not just to know who an individual is or where they are, but to then take that information and use it to control or otherwise direct their actions. The agent of this mode of power in this context is the police/law enforcement officer or department utilising AFRT. This kind of power is generally accessible to anyone who has access to AFRT. However, in this context as we are looking at how police and law enforcement agencies use AFRT, the agent(s) are those officers or departments using AFRT.

The subject of power in this context are persons of interest to the authorities. This is a broad category of subjects and will be different depending on the ways in which this technology is used by law enforcement officials. In many cases, the subject will be someone specific, such as a suspect being actively pursued by police officers. In others, the subject will be anyone within a crowd of people who may be identified by authorities as a threat, such as someone in a crowd at a protest who may be becoming violent. In still other situations, the persons of interest will be a group of persons, or even a whole population, as is the case with the use of AFRT in China to target the Uyghur population. Whether the subject of power is a specific individual or a group, the operation of AFRT is to effectively end anonymity in public spaces, to make the crowd irrelevant. AFRT looks through the crowd and identifies persons of interests for power to target, where before big data those persons of interests could hide from the operation of power.

There are two main techniques or mechanisms that make up the means of power in this context. The first is the use of identification through biometrics. Just as with the operation of China's social credit system and Amazon's workplace management technologies, there is an essential element of mass surveillance, but the mass surveillance here is combined with biometric information to create a form of surveillance that is both more targeted and vastly more comprehensive. Though a crowd may be surveilled, the use of biometric information in the form of facial recognition is the crucial method by which power operates in this context. The second mechanism of power here is the threat of force or sanctions from police or other law enforcement officers and agencies. Once the individual has been identified, it becomes possible for the relevant law enforcement officer or agency to threaten force or some other sanction against that person. From the perspective of an arrested individual, the form of coercive power exercised by police forces is substantially the same as it was before AFRT. However, this technology radically extends the scope and range of these coercive powers by making them increasingly inescapable. The effectiveness of the threat of potential punishment is greatly amplified as the likelihood of being caught approaches certainty.

For Dahl, the claim that a particular exercise of power, such as a police order, causes an outcome is substantiated by a counterfactual observation about what would have happened if not for that exercise of power:

> *... suppose a policeman is standing in the middle of an intersection at which most traffic ordinarily moves ahead; he orders all traffic to turn right or left; the traffic moves as he orders it to do. Then it accords with what I conceive to be the bedrock idea of power to say that the policeman acting in this particular role evidently has the power to make automobile drivers turn right or left rather than go ahead.* (Dahl 1957, p. 202)

In the context of police or law enforcement agencies using AFRT, the operation of power is aimed at causing identified individuals to do something that they would not otherwise do, such as attend a labour camp, submit to an arrest, or otherwise act (or refrain from acting) in a certain manner. Coercive and causal power is exercised to force an individual do something they would not otherwise do. Importantly, this is only possible because of the conflict of desires in the social relationship between the police and the general population, which is a key feature of Dahl's account of power. For those individuals who do not feel the exercise of power in this context, their desires and interests largely align with those of the police, while those who are subject to exercises of police power here have some conflicting interest or desire. That may be a desire to act in a way that is unlawful, and thus the police have a conflicting desire to prevent crime, or as in the case of the Uyghur population the desire may be for autonomy and self-governance, which conflicts with the political goals of the Chinese government.

In this context, the use of AFRT is an important part of the base of Dahlian power. The base, or the source of power, is made up of the different resources that can be exploited as part of exercising power. AFRT is an essential resource that the police can rely upon for exercising power in this context. There are of course other bases in this context which go towards providing a source for power. These bases could include the possession of weaponry or other equipment that could be used as part of the exercise of power, the legal authority to issue fines and make arrests, and acceptance of their legitimacy by the population.

A base of power is inert until it is exploited in some fashion, and as AFRT is used, this base of Dahlian power is exploited as part of the means of power. It is important to note here that I am following Dahl in using the term "means" when describing the operation of power. Dahl uses this term to describe either the exploitation of a base of power, or a kind of mediating activity between *A* and *B* such as a threat or promise. This is not inconsistent with how I conceive of the idea of the means of a mode of power, namely the mechanisms, techniques, and practices by which a mode of power acts on its subjects in pursuit of its goal. In this context, though AFRT makes up part of the base of power, as Dahl constructs power, its use in identifying individuals and the making of a threat of force or other sanction against that individual then acts as the means of power.

Following Dahl’s method, the operation of power can be discovered using counterfactual reasoning. Power has been exercised when an agent possessing power makes the subject do something he or she would not otherwise do. Coercion and sanction, and the *plausible threat* of coercion and sanction are, in Dahlian terms, ‘bases of power’, and constitute power in its most intuitively recognisable form. I have argued that AFRT is a technology that radically extends and amplifies these bases of power, and that it is instructive to apply a Dahlian framework to the use of AFRT in policing.

Pandemic Tracking

In December of 2019, the Wuhan Municipal Health Commission in China reported a cluster of cases of pneumonia in Wuhan, the capital of Hubei province (WHO 2020). At the time, the cause of the cluster was unknown, but eventually a novel coronavirus outbreak was identified. The first case outside of China was identified in Thailand on 13 January 2020, and the disease spread rapidly from there, with cases appearing in 18 countries by the end of January, and the disease caused by this novel coronavirus was named COVID-19 in early February. The World Health Organization declared COVID-19 a pandemic on 11 March, and by 4 April there were over a million cases of COVID-19 across the world, more than a tenfold increase in less than a month. By the end of December 2020 there were over 70 million cumulative cases of COVID-19, and over 1.6 million deaths worldwide (World Health Organization 2020).

As part of the effort to contain the spread of COVID-19, many governments and private entities looked to big data. Broadly speaking, we can identify three categories of use for big data in response to COVID-19, modelling, documentation, and contact tracing (Wong 2020). In terms of modelling, a wealth of geolocation data is being used to construct models of both the spread of the virus and the impacts of policies and strategies put in place by states to contain the virus. While individual states are often doing much of this modelling themselves, private companies are also providing access to their databases for use in modelling. Google has launched their COVID-19 Community Mobility Reports (Fitzpatrick & DeSalvo 2020), to track changes in the way that people in communities move around as a consequence of the pandemic. These reports cover over 130 countries, including individual states or provinces within those countries, and indicate changes in movement across different areas such as public transport, retail stores, parks and public areas, and workplaces. Facebook has released a series of maps and publicly available mobility datasets to help health authorities model the spread of COVID-19 and measure the effectiveness of local policies (Jin & McGorman 2020). Some of the modelling that Facebook is providing includes tracking movement ranges over time, showing at a regional level whether people are staying close to their home or visiting a number of places across a city, social connectedness indexes, showing the number of social connections between different cities and regions to indicate where outbreaks might spread to, and co-location maps, which indicate the probability that people in an area will come into close contact with each other.

The second use for big data in combatting the spread of COVID-19 is in mapping and tracing the past movements of individuals. When data is used for larger scale modelling, it is less important who the people doing the moving are. When data is used for contact tracing or quarantine enforcement, for example, the main concern is the precise movements of individuals. Generally, when data is being used for this purpose it is to ensure that individuals are remaining in mandated isolations or quarantines, or in some cases it is to document who has become infected with COVID-19 (or are at least are showing symptoms of infection). Various governments across the world have adopted data driven technologies to do this, especially several countries in Asia. The Taiwanese government was an early adopter of this kind of mapping and tracing, as they implemented QR code scanning to report travel history as early as 5 January (Duff-Brown 2020). Those travelling to and from Taiwan (including the 850,000 citizens who live in mainland China and the 400,000 citizens who live in Taiwan and work in mainland China) are required to scan QR codes to report their travel history. Those who had travelled to high risk areas are required to go into a minimum 14-day self-quarantine at home. Compliance with this quarantine period is assessed by monitoring phone usage including geolocation data. Hong Kong adopted similar measures for monitoring of isolation requirements, with residents who are required to self-isolate instructed to add local authorities on WhatsApp, a communication app developed by Facebook, and to share their location with those same local authorities so their movements can be documented (Wong 2020).

China is also using big data to document the movements of individuals across the country (Yuan 2020). Alongside tracking mobile phones like in Taiwan and Hong Kong, China is also utilising its extensive network of CCTV cameras and AFRT capabilities. Key points across China such as train stations and the entrances to markets are equipped with thermal imaging devices which are linked to the AFRT system. If an individual displays a raised body temperature, one of the early symptoms of COVID-19, then AFRT will identify that individual. Individuals who register a high temperature can be contacted and directed to get tested and/or self-isolate, and others who have been in contact with those individuals can also be identified and directed to get tested and/or self-isolate. China also appears to be using this technology to monitor compliance with orders to self-isolate at home, as residents of Hubei reported in January that they were contacted by authorities when leaving their homes before their period of self-isolation was finished. It is claimed that local authorities are using AFRT to detect individuals who are supposed to be at home and are then directing them to return home as soon as possible or risk fines.

In those countries whose governments have implemented social distancing requirements, private groups and businesses are also turning to big data to help evaluate how their employees and customers comply with these requirements. Some businesses have turned to AFRT to track and monitor their employees (Metz 2020). AFRT is being used to monitor whether employees are wearing masks or not, and to monitor employee movements and proximity. It can detect whether employees have spent too much time in close proximity, or if they are walking on a trajectory that will lead to close contact. Other companies are using infrared technology to track and scan movement through doorways to monitor occupancy in a space as well as the speed and direction of the movement of individuals (Wiggers 2020). For these businesses, while the use of infrared scanning doesn't allow for the identification of individuals, it allows for occupancy tracking in places where security cameras cannot go such as bathrooms or dark rooms in nightclubs.

The third general use of big data is in contact tracing. To help curb the spread of COVID-19, and to maintain an accurate picture of the extent and location of any outbreak, health authorities across the world are tracing the movements of infected individuals to identify those they have been in contact with. Many countries are using big data to make this process easier and faster. There are two approaches to using big data to augment contact tracing efforts, a top down or centralised approach and a bottom up or decentralised approach (Wong 2020). Top down approaches involve government bodies or agencies directly aggregating data about individual's movements. One country utilising a top down approach is South Korea, where automated systems collect data from various systems around the country's smart cities for use in contact tracing.

More common are bottom up approaches, using phone-based Bluetooth tracking. Over 30 countries have developed or are developing contact tracing apps, and major phone operating systems develops such as Google and Apple have rolled out contact tracing functionalities. These apps function by assigning a randomised ID to the phone the app is installed on, and when two or more phones spend an extended period of time (usually between 15 and 30 minutes) in close proximity those IDs are exchanged using Bluetooth functionality. If a user tests positive for COVID-19, they can then release that information into the notification system or to local health authorities (depending on the functionality of the app itself) to then notify other users who have been in close contact with the infected individual prompting them to get tested.

Power in Pandemic Tracking

While there are several different ways that big data can be used in the effort to combat the spread of COVID-19, we can still identify modes of power across these various uses. The goal of power in this context is, to put it simply, the suppression or elimination of disease. More specifically, the disease in question is COVID-19, but it is easy to picture a scenario where the target is a different infectious disease. While ultimately this will result in a generally healthier populace, the goal of power here is not to ensure the health of the population, but to suppress or eliminate a particular affliction. The agent of power here is the government or some state health authority. While there may be cases where others, such as private businesses or individuals, are utilising the data driven technology discussed above, and thus may appear to be the agents of power here, that is not really the case. The intentional agent behind the operation of power in this context is the government or a state health authority, and any private business or individual who then uses these technologies is either acting in concert with or in response to the exercise of power by the agent behind power in this context.

The goal of power here is to eliminate the virus, but power cannot act directly on the virus and so must act on human beings as hosts, vehicles and transmitters of the virus. Regarding these human subjects of power, it is important to then distinguish between those who are infected and those who are not yet infected. We can identify these two different classes of subjects as this mode of power operates differentially on these groups. Those who are infected may find they face stricter restrictions and more stringent punishments for flouting those restrictions, whereas those who are not yet infected are required to observe hygiene and social isolation measures to avoid becoming infection.

There are a variety of means for this mode of power, largely in line with the variety of uses for big data in tracking and suppressing the spread of COVID-19. Across the various uses however a consistent technique is the operation of surveillance. Modelling, documentation, and contact tracing all require a constant level of surveillance on a variety of individuals and for a variety of purposes. For surveillance purposes, mobile phones are the primary source of data. Automated contact tracing relies on the ubiquity of mobile phones, but most forms of modelling and documentation similarly rely on collecting geolocation data from the use of mobile phones. Beyond the use of surveillance, another important technique for this mode of power is the threat of sanctions such as fines or imprisonment. While some individuals may comply with power purely out of fear of contracting COVID-19, the behaviours demanded by the agent of power in this context are enforced with legal penalties, such as fines.

Which theoretical accounts of power are applicable to this context? While in the contexts of the Chinese social credit system and police use of AFRT there is a clear overlap with one theoretical account of power, and at Amazon there is an overlapping of two accounts of power, in this context we can see features of three different accounts of power, namely Parsons', Foucault's, and Hobbes' accounts. These accounts both overlap and operate in parallel to each other in this context, in a kind of elaborate and dense network of different kinds of power. A pluralistic attitude towards power and the more focused questions discussed in the previous chapter are valuable in contexts such as these as they allow us to see where and how different conceptual kinds of power overlap and interact as different modes of power.

First, we can see key features of Parsons' account of power. Across many of the pandemic measures being introduced by various governments and health authorities, there are agents controlling the direction of social action, particularly with respect to documenting the movements of individuals. A clear example is the use of QR code scanning in Taiwan to track where individuals have recently travelled. Within the structure of a large and complex system, namely the borders of countries, the compliance of individuals is being purchased by the government. By offering the reward of faster travel (inducement) and threatening the punishment of exclusion or isolation (coercion), the government as the agent of power here is controlling or directing decisions individuals make about their movements.

We can also see conceptual features of Foucault's productive power, overlapping with and forming a kind of hybrid with Parsons. One of these key features is that power operates across innumerable diffuse points rather than from one centralised source, and in this context we can see exercises of power that function in this exact way. The extensive surveillance networks used here are spreading power out across the system, so that power is being exercised across diffuse points in the relationship between government or health authority and citizen. As mobile phones are turned into tracking devices, tracing movements and monitoring who is nearby, the exercise of power is spread out across the system. Further, the surveillance that individuals are being subjected by is an overt kind of surveillance, prompting the kind of self-regulation that is a characteristic feature of a Foucauldian productive power.

Finally, features of Hobbesian power are also present in this context. In many countries and regions, governments have resorted to harsh lockdown measures, forcing individuals to remain within their homes and only allowing trips to get essential supplies like food (and in some regions only allowing those trips on a rigid schedule). In the implementation of these lockdowns we can see the naked force of a causal, Hobbesian power. The State is exerting a causal force on the population to make them stay inside, using the threat of force in the form of imprisonment or fines to achieve the desired end effect of a lockdown. Indeed, lockdowns are being used in many places as threats in and of themselves to back up other containment methods that can be understood as Parsonian or Foucauldian. In this context, there is a base level of Hobbesian power sitting in the background, waiting to arise as a direct causal force controlling the population through the power of the leviathan.

The use of big data to track the spread of COVID-19 is a difficult context to analyse using a unitary approach to power. Attempting to assess this context through the lens of only one theoretical understanding of power will lead to important details being downplayed or missed entirely. However, by adopting a pluralistic attitude towards power we can see the key features of causal, procedural, and productive understandings of power, which in turn gives us a more nuanced and detailed understanding of how power is exercised in this context, and how big data is used as a technology of power.

Conclusion

Big data, or more accurately the bundle of technologies that make up big data, can be used in many different ways across different contexts, and to properly understand how it is used as part of the exercise of power it is essential to begin by identifying the modes of power operating in those contexts. The examples above, of the Chinese social credit systems, Amazon’s workplace management technologies, police use of AFRT, and official’s responses to the COVID-19 pandemic, illustrate the necessity for a pluralistic approach to understanding power. By identifying the goal, agent, subject, and means of power we can grasp how power is operating in that context and how big data is being used as part of that exercise of power.

In the case of the Chinese social credit system, we can see many of the key conceptual features of Foucault’s account of power, as big data is used to track and rate citizens and consumers, to then make decisions based on their trustworthiness and further mould them overtime to be better subjects of power. In the context of Amazon’s use of big data to manage the workplace, we can see key features of Foucault’s productive power and Parsons’ procedural power overlapping with each other, as the decisions of employees are controlled by management as they are shaped to be ideal subjects of power. As the police use AFRT to track and monitor individuals, they are using big data to facilitate decision making around who is subject to police intervention in ways that neatly align with the conceptual features of Dahl’s account of power, where the police cause individuals to act in ways they otherwise would not. Finally, in the context of the COVID-19 pandemic, governments and health officials across the world have utilised a range of big data driven tools to exercise power in a variety of ways, displaying features of Foucauldian, Parsonian, and Hobbesian understandings of power all with the general aim to track and control the spread of the virus.

These four cases are prime examples of the ways in which big data can be picked up and used to facilitate and automate decision-making processes, and thus be used in the exercise of power. However, as big data is used in the exercise of power, it also has a transformative effect on that form of power. There is something that is different, for example, in the operation of Foucauldian power through the social credit system than in the contexts that Foucault was first considering when he set out his account of power. In the following chapters, I will explore these differences, with an aim of bringing both more subtle and more revolutionary changes into focus.

Chapter 5

Historicising Big Data

In the previous chapter, I showed how a pluralistic attitude towards power is useful for developing a more nuanced understanding of different modes of power that may be present in different contexts. In the four examples discussed, the Chinese social credit systems, Amazon's workplace management, the police use of AFRT, and pandemic tracking, the use of big data is a major part of how power operates. However, to fully understand how big data is used as a technology of power it is also important to examine the effects of big data on the exercise of power. It is evident that big data has, in various ways, changed how power is exercised and used, and the following three chapters focus on examining these changes and impacts on the operation of power.

This chapter expands upon a claim made in Chapter 3, that the analysis of how big data tools are applied as instruments of power does not require a new theory of power. Against the view that big data has ushered in a novel and unprecedented form of power, this chapter discusses important historical continuities in the operation of power today and in pre-digital times. While big data has had a significant impact on power, this impact is in many ways comparable to the social transformations caused by other technological developments throughout history. We should be sceptical of claims that the emergence of big data marks a historical break, and instead pay attention to historical continuities that are relevant for understanding the contemporary impacts of big data. By paying attention to these historical continuities, we can more precisely describe the impacts of big data on the operation of power, and in turn how the use of big data as a technology of power can violate normative concepts such as equality and autonomy.

To demonstrate these important historical continuities, I will look at four historical contexts, and compare them to those in the previous chapter. These comparisons show that, in otherwise very different times, we can see the same modes of power at work. First, I will look at the reforms of the Fourth Lateran Council of the Roman Catholic Church and show that we can see the same features of Foucauldian power present as in the context of the Chinese social credit systems. Second, I will examine the *cursus publicus*, the Ancient Roman road and postal network, where similar features of Parsons' and Foucault's accounts of power are present, as in the context of Amazon's workplace management techniques. Third, I will examine the development of police fingerprint databases in the late 19th and early 20th centuries to show that the kind of Dahlian power exercised in the police use of AFRT emerged at least a century ago with the development of analogue databases for policing. Fourth, I will compare French plague regulations from the 17th century with the use of big data to track the spread of COVID-19, as these cases are comparable with respect to features of Parsons', Foucault's, and Hobbes' accounts of power.

The comparison of these historical and contemporary contexts suggests that the use of big data does not necessarily change the nature of power. However, as with other new technologies, the use of big data does impact on the exercise of power, and the differences in these contexts help to highlight some of these impacts. Big data technologies can make the exercise of power more efficient or cost-effective, and they can increase the range, scope and forcefulness of power. The final section of this chapter explores some of these significant impacts on the operation of power.

The Big Data Age

A common approach to the relationship between big data and power in the literature characterises big data as part of a technological revolution that has radically transformed the operation of power, perhaps even to the extent of ushering in an epochal shift. While big data certainly has had an impact on the operation of power and will continue to change how power is exercised and experienced, it is a mistake to represent these transformations as unprecedented.

Recall the discussion at the start of Chapter 3, summarising the work of several writers who have considered the relationship between big data and power. We can group these writers roughly into two main camps. The first are those who argue that the development of big data has driven a shift from a Foucauldian disciplinary society towards a Deleuzian control society. This group includes Cheney-Lippold (2011), Thompson (2016), and Matzner (2017), amongst others. While they differ on the causal mechanisms of this shift, they agree that the rise of big data has led to a shift in how society is structured. A more radical approach can be found in writers who argue that the development of big data requires us to develop completely new theoretical understandings of power, such as algorithmic governmentality (Rouvroy 2016; Rouvroy & Berns 2013), smart power (Han 2017), metric power (Beer 2016), and instrumentarian power (Zuboff 2019). While I do not deny the considerable value of these analyses, my aim here is to demonstrate that focusing on historical continuities and similarities, rather than discontinuities, can also be instructive.

What follows is a discussion of four historical examples which parallel the examples of the previous chapter. In each case the aim is to show that the same modes of power seen in the contemporary 'big data' examples have, in the past, been served by pre-digital technologies. First, we look at the connections between the Chinese social credit system and the reforms of the Fourth Lateran Council of The Roman Catholic Church in 1215. Then, we examine the similarities between the operation of power in Amazon's workplace management technologies and along the *cursus publicus*, the Ancient Roman postal network. Third is a tracing of the history of police surveillance to compare the use of AFRT and early fingerprinting at the end of the 19th century. Finally, we consider the similarities between the contemporary response to COVID-19 and regulations used to stop the spread of plague in the 18th century.

Social Credit and the Roman Catholic Church

The operations of the Chinese social credit systems bear striking similarities to the practices of the Roman Catholic Church of the Middle Ages. The Roman Catholic Church (the Church) is the world's oldest continuous international organisation and was at the height of its political influence throughout the Middle Ages. From the fall of the Roman Empire, there was significant growth in monasticism throughout Europe, and the monasteries became centres of religious, cultural, and scholastic life across the many warring kingdoms and states of Europe. Over time, and helped by the cultural importance of the monasteries, the Church rose in prominence to become the most influential political force in Europe. By the 10th century, the cultural and religious notion of Christendom began to develop (Cunningham 2020). Christendom, which generally refers to the "Christian world", played a central cultural role in Europe from the 10th to the late 13th/early 14th centuries. For many living in Europe, their cultural identity as a member of Christendom was often more important to them than their membership of a kingdom or feudal state.

At the height of their cultural and political influence in the early 13th century, the Church adopted a number of reforms (Power 2016) in an attempt to eliminate heresy and to normalise the practice of religion across Christendom. For the purpose of this discussion, the most important reforms are two of the resolutions adopted during the Fourth Lateran Council in 1215, aimed at rooting out heresy (Deanesly 1969, pp. 139-140). The first resolution required all archbishops and bishops, or their representative archdeacons, to hold annual inquisitions. Clerics would, on a yearly basis, "inquire" as to the existence of any heretical teachings, compelling witnesses to testify on oath as to the existence of any heretics or secret "conventicles". In practice, the cleric or inquisitor would visit a town and compel the inhabitants to accuse all those they suspected of heresy. Those who were accused would then either plead guilty and perform penance, or plead innocent and (usually) suffer far harsher punishments including torture or even death (Deanesly 1969, p. 217). These inquisitions were often assisted by spies the Church had embedded in the region, as well as by townspeople, who were regularly encouraged by the Church to report neighbours suspected of heresy to local clerics.

The second important reform for present purposes was the institution of confessionals (Deanesly 1969, p. 140). Individuals were required to confess all their sins to a local priest at least once a year (preferably more frequently) and to perform any penance prescribed by that priest. While the inquisitions looked to stamp out heretical views of Christianity (i.e. versions of Christianity not approved by the central Church), these confessionals compelled individuals to confess all other miscellaneous sins. Although the tradition of "auricular confession" (i.e. the confessing of sins to a priest) predates the reforms of the Fourth Lateran Council (Cunningham 2020), the resolution of the council cemented it as one of the major sacraments of the Church. To this day it is still mandatory for all practising Catholics to undertake the Sacrament of Penance (confession) at least once a year, though they are also still encouraged to perform it more regularly.

The goal of power that these two reforms were aimed at was to strengthen the cultural and religious control of the Church through both rooting out heresy and making religious salvation dependent on confessions. While power here was in practice carried out by individual clergy members, the agent of power here is the Church as a broader organisation, and its subjects are the members of Christendom. The means of this mode of power are the use of punishments for those who fail to live up to the standards of Christianity as set by the Church ranging from simple penances to physical torture, the use of surveillance through Church-sponsored spies, regular inquisitions, and turning neighbours into informants, as well as imperatives to self-report through confession.

The method of enforcing the Church's power by imposing a generalised surveillance designed to identify and publicly shame or punish those who deviate from prescribed orthodoxy resembles the mode of power at work in the Chinese social credit systems. Many of the key features of Foucauldian power are present in both contexts. While the Church exercised power through punishments, the aim of these punishments was to develop parishioners over time to be idealised subjects of power. These parishioners then saw themselves not as members of individual kingdoms, but as members of Christendom, defining themselves through the relationship they had with the Church. Regular and enforced confessionals and inquisitions functioned as a kind of overt surveillance, training parishioners to self-regulate and become better subjects of power. The exercise of power both defined and was defined by the nature of the relationships between parishioner and clergy and was felt as a diffuse force across the relationship, especially as people were encouraged to assist in inquisitions by turning in their neighbours for heresy. While the Church did not have access to the technology available to the Chinese government and companies, they both exercised a kind of power with the same key conceptual features.

Of course, there are differences between the operations of the Church in the early 13th century and the operations of the Chinese government and corporations in the early 21st century. The Church had to rely on physical, in-person, surveillance, and as such their power was limited. Parishioners were encouraged to watch each other, training each other to be part of the surveillance that was crucial to the exercise of power by the Church. The Chinese government and those corporations who use big data to run social credit systems have far more advanced surveillance tools at their disposal. They can use surveillance that is far more efficient in terms of economic and time costs, and far more effective than physical surveillance as a much more diverse range of information can be tracked, and in much finer detail. The mode of power deployed in these cases is fundamentally the same, despite the technological differences. Indeed, it is significant that, even with ubiquitous automated surveillance and data analytics, the Chinese government still relies on neighbourhood informants, arguably because it is a powerful strategy for undermining the development of anti-government solidarity between citizens. The emergence of big data technology has not (as some authors have claimed) made Foucault’s disciplinary conception of power obsolete. Rather, in contexts where disciplinary power operates it is now enhanced by new surveillance capabilities. It is important to recognise, however, that the elements of disciplinary power can also be found much earlier than the historical period examined in *Discipline and Punish*. Indeed, for Foucault, certain aspects of disciplinary power originate in the religious practice of confession (Deacon 2002). The point of the comparison between the Chinese social credit systems and the practices of the Church of the 13th century is to show that the adoption of new technologies, as instruments of power, does not necessarily constitute a new form of power. In its essential elements, the mode of power exercised today by means of a social credit score can be found in medieval Europe.

Workplace Management and the *Cursus Publicus*

The Roman Empire, as one of the largest empires of antiquity, was faced with the pressing issue of maintaining its control over a vast area. At its height, the Roman empire extended over 4.4 million square kilometres (Taagepera 1978, p. 117), stretching from the northern tips of Britannia at Hadrian’s Wall, to the western edges of Europe and modern Morocco, Egypt in the south, and across Mesopotamia and Assyria in the east. By foot, travel to Roma from Constantinopolis would take 21 days, from Londinium and Coptos 27 days, and from the furthest reaches of Britannia or East Mesopotamia over a month (Scheidel & Meeks 2012). Even at fastest speeds by using a relay of horses across the great Roman roads, the 1,694 km trip from Constantinopolis would take 7 days, and the 2,081 km journey from Londinium would take over 9 days (Scheidel & Meeks 2012). To maintain its control over the empire, the Roman government developed complex systems of surveillance that would not be matched until hundreds of years later.

The Roman military played a key role in this system of mass surveillance. Outside of their functions in armed conflicts, soldiers performed various roles across the empire such as guarding state depots, escorting transports and couriers, performing police duties along major roads, and acting as state authorities along the edges of the empire (Herz 2007, p. 307). However, more important than the performance of the surveillance itself was the transmission of gathered information and other goods from the furthest regions of the empire back to Rome. The Romans achieved this impressive logistical feat through their postal system, the *cursus publicus*. The *cursus publicus* was not the first postal system to be developed, with evidence of similar systems in Egypt around 2000 BCE, China around 1000 BCE, and the Persian Empire from the 6th century BCE (Brix 2020), and the Romans under Emperor Augustus (27 BCE to 14 CE) borrowed elements from the Egyptian and Persian postal systems to develop their own. The *cursus publicus* operated over the next several hundred years, and only began its decline after the separation of the West and East Roman Empires (Kolb 2001). While it declined more rapidly in the West following the sacking of Rome by the Visigoths, elements of the system remained operational in the East until the fall of Constantinople in 1453, and the system remained largely unmatched in efficiency and scope until the 19th century (Brix 2020).

The *cursus publicus* was itself a series of relay stations or posts at key intervals along the great Roman roads. The posts were divided into two types, *mansiones* that included lodgings and replacement animals, and *mutationes* for simple exchanges of animal teams during a day’s travel, with smaller stations at intervals of 20-30 miles apart and larger stations between 100-150 miles apart (Kolb 2001, p. 97). At these stations, a variety of animals were kept for transportation purposes, with horses typically used for faster despatch rides, mules used as draft animals for slightly slower carriages, and oxen for heavy freight. The most common cargo to travel through the system were war materials, and parchments and papyrus with state information and revenue. While responsibility for the *cursus publicus* ultimately lay with the Emperor, the costs of the system (in terms of animals and supplies) would have been overwhelming for the empire (Kolb 2001, p. 96), and so were largely imposed on those who lived along the routes of the *cursus publicus*.

The costs of running each station were borne by the *manceps* or *praepositus* who oversaw it. These costs included paying for the numerous staff needed, as well as the upkeep and replacement costs of livestock, and in many cases materials for additional services, such as cart repairs or horse-shoe replacement. Being appointed as *manceps* of a station could bankrupt even the wealthiest of families, and there are records of individuals going to great lengths to avoid being appointed. In some extreme cases, individuals would get themselves arrested, marry their own slaves, or vanish from society to live as a hermit (Kolb 2001, p. 99). For those that remained as *manceps* and did not run off into the woods, there was also the opportunity to siphon funds from the system. Much of the cargo that travelled through the *cursus publicus* was essential to the operation of the empire and included valuable goods as well as records of those goods. Unscrupulous *manceps* found themselves in an ideal position to bolster their own resources by siphoning off some of the wealth that travelled through the system.

While the costs of the system were largely borne by those operating it, responsibility for the *cursus publicus* rested with the Emperor, and so the Emperor needed to ensure its smooth operation. Over time, a complex bureaucracy developed to oversee the *cursus publicus*. Initially, army quartermasters or *frumentarii* administered the system, ensuring that cargo travelled without interruption and those charged with running the system performed their duties. But as the system grew in size and importance, it needed more and more dedicated oversight, including militia forces, local magistrates, centralised accountants in Rome, and a large secret police force travelling along the roads themselves (Kolb 2001, p. 100). At its height in the second half of the 5th century CE, there were 1,248 agents managing the system, with many of those agents watching each other. Those who performed well were rewarded, with *manceps* in particular receiving tax concessions and other benefits to ensure they performed their duties. Those who shirked their duties or were caught siphoning from the system for personal gain were punished harshly by the Empire, often based on the information gathered by the secret police.

In the context of the *cursus publicus*, the goal of power is to maximise income; to extract the maximum value from citizens and territory while expending as little money and resources as possible. In this context, this income predominantly takes the form of taxation. The agent of power here is the Roman government, acting either through the officials in a region or through the bureaucracy of the political structure. While the *cursus publicus* impacted on the lives of most citizens in the Roman Empire, the subjects of power in this context are those who live along the road system, particularly those who are charged with running and maintaining it. The operation of power here is aimed at those individuals as its targets, as changing their behaviours was necessary for achieving the goal of power. In regard to the means of power here, surveillance of the *cursus publicus* and those who live along it was an essential technique, as well as the limiting of options and the offering of incentives to those who refuse or comply in running the *cursus publicus*.

At first glance, it may seem that there are more differences than similarities between the *cursus publicus* and Amazon’s workplace management technologies. Leaving aside the technological differences, Amazon is a private business where the *cursus publicus* was a government administered system, and income takes the form of profit for Amazon, as against taxation for the *cursus publicus*. As such, it might seem counter intuitive or anachronistic to compare the two contexts. However, if we abstract away from these differences, we can nevertheless identify the same conceptual features of power in each context.

Power, here, is again operating in a productive rather than a merely repressive fashion, a key feature of Foucauldian power. The *manceps* and assorted officers placed in charge of the *cursus* *publicus* would be trained and shaped over time to be idealised subjects of power; better officers of the system that were more responsive to direction by the State. This was in part encouraged by constant, and mostly overt, surveillance of the system. While some of the surveillance was covert, such as the surveillance performed by the secret police, there were other forms of surveillance that were overt, such as inspections by army quartermasters and other State agents as well as systems of punishments and rewards which relied on regular information coming in. While the surveillance performed by the Roman Empire was far less comprehensive than that performed by Amazon today, for the time it was relatively constant and extended to all aspects of the system's operation across a vast geographic area.

Recall the key features of Parsonian power, namely that power works to secure the performance of obligations, that power in complex social systems must be legitimised within that system, and that power can be exercised through any one of four strategies. These features are also present in the context of the *cursus publicus* just as in the context of Amazon's use of big data. The *manceps* and other citizens who are charged with running the stations along the *cursus publicus* frequently had their decision making overruled by the Roman State, indicated by the evidence that many chosen for that "honour" attempted to avoid the duty imposed on them. The stations had to be run in particular ways, or else the *cursus publicus* would fall apart, and an elaborate system was developed over time to surveil and account for the operation of the stations along the Roman roads. The power of the Roman state to have their decisions override the decisions of those running the system was legitimised within the broader context of Roman society, and we can clearly see the four strategies of Parsonian power, that is, inducement, persuasion, coercion, and the activation of commitments as officials controlled the actions of those running the system, with a combination of punishments and rewards. If Amazon appears in some ways to resemble an imperial power in its operations, that may be because it enforces operating standards in its global distribution network in ways that resemble Rome's administration of its distribution network.

Just as the development of big data has not made Foucault's account of power redundant or obsolete, it has also not made Parsons' understanding of power irrelevant. It also has not changed the nature of power between these two contexts, including the ways in which these two kinds of power overlap with each other. As Amazon's employees are being trained and shaped to be ideal workers through control over their decision making, so too were the *manceps* controlled and trained by means of a kind of hybrid operation of Foucauldian and Parsonian power. The primary difference between the two contexts is that the use of big data allows for direct control over decisions and actions to be exercised in far more fine-tuned and fine-grained ways.

Facial Recognition and Fingerprints

Fingerprints have long been recognised as being unique to each individual, and we have evidence that ancient societies used fingerprints as signatures. Imprints in pottery and clay bricks and tablets circa 3,000 BCE from Mesopotamia and Egypt suggest craftsmen used fingerprints as marks of their work (John Berry 2001, p. 25), while a Chinese clay seal from sometime before the 3rd century BCE shows a thumbprint alongside a written signature, suggesting the use of fingerprints as official signatures (John Berry 2001, p. 26). The Persian historian Rashid al-Din commented on the use of fingerprints as a method of authentication in China in 1303, remarking that ‘Experience shows that no two individuals have fingers precisely alike.’ (Cole 2002, p. 61). While the idea of fingerprints denoting some kind of individual stamp of identity was widespread in the ancient world, the first known detailed study of the ridges, furrows and pores on both hands and feet was produced by the English plant morphologist Nehemiah Grew in 1641 (John Berry 2001, p. 27).

Before discussing the development of fingerprinting in policing, it is useful to briefly cover some of the history of the modern police force. Before the late 18th and early 19th centuries, police forces were largely localised and often consisted of conscripted militia. One of the first professional police forces, the Metropolitan Police Service (the Met), was established in London by Sir Robert Peel in 1829. A key innovation of the Met was the assignment of police to allocated “beats”. This innovation was developed specifically as a kind of surveillant machine (Williams 2003, p. 28). One of the key functions of the beat police was to monitor and patrol defined areas, paying special attention to ’rogues and vagabonds’, including reporting to superiors on the numbers of known thieves and depredators, prostitutes, suspected persons, vagrants and tramps, as well as houses of bad character and other resorts of thieves and prostitutes observed within the areas they patrolled (Williams 2003, p. 29). The Met were world leaders in policing, and many of their techniques, including the beat police patrols, spread worldwide.

The surveillance the police provided however was expensive and had substantial gaps. The initial budget for the Met police in 1829/1830 was £194,126 (approximately equivalent to £21.5 million today) which quickly doubled to £437,441 (£52.4 million) in 1848, and then £1.8 million (£235.7 million) by 1898 (Fido & Skinner 1999, p. 56). To bring rising costs under control, and increase efficiency, police forces turned to developing scientific identification methods, including fingerprinting, to streamline operations. Increasingly, English police forces began to track known criminals and ex-prisoners by means of registers, such as those established through the Habitual Offenders Acts of 1869 and 1871 (Williams 2003, p. 29). These and similar registers were intended to provide a more rigorous and scientific method for easily identifying known criminals should they reoffend. Around the same time, there was growing interest in the use of fingerprints for identifying people. There were several competing systems being developed at the end of the 19th century, but the one that rose to prominence in the English-speaking world, and is still used today, is the Henry system.

Edward Henry was a colonial officer in India and was responsible for overseeing what was essentially a local pension system. To combat fraud in the region, a previous administrator named William Herschel had adopted a local custom and was using palmprints and fingerprints to reduce or eliminate the chances of someone claiming multiple pension benefits (Cole 2002, p. 65). Herschel recommended that a similar system be adopted by police forces, but his recommendations were not taken up. Henry, who had dealt with Herschel’s system, also felt that the police should use fingerprints to identify criminals, but he needed to develop a classification system to standardise the process. So, he tasked two of his clerks (Khan Bahadur Azizul Haque and Rai Bahadur Hem Chandra Bose) with developing a classification system that allowed for easier analysis and crossreferencing of collected fingerprints.

There are two kinds of fingerprint analysis, fingerprint verification and fingerprint matching (Jiang 2015, p. 585). Fingerprint verification is a process where a sample fingerprint is compared against a stored print and is typically used as a form of key access for doors or electronic devices. Fingerprint matching is a one to many process, where a sample print is compared to a larger database to find a match and identify the sample owner. It was the ability to perform fingerprint matching that Henry's system allowed for, and initially police departments in India used the system to identify and track prisoners and known criminals. In 1898, the system was used for the first time as part of a criminal investigation and faced its first big test when it was used as evidence in court for the identification of a suspect in a murder trial (Cole 2002, p. 89). While the defendant was acquitted on the charge of murder, the judge in the case was satisfied that the partial print left on a wooden box placed the defendant at the scene of the crime, and thus found him guilty of burglary. Following this success, the Met adopted the techniques and began a trial of fingerprint analysis in 1902. In its first year of use, they made 1,722 identifications through fingerprint analysis, far surpassing any previous systems, and by 1904 they were processing over 350 new fingerprint sets every week (Cole 2002, p. 94). By 1950, the Met had over one million fingerprints on file (Williams 2003, p. 29). Fingerprinting quickly spread to other countries, including the US, Canada, Argentina, Australia, New Zealand, and much of Europe, by the early 20th century.

In terms of the operation of power, the mode of power exercised in contemporary police forces use of AFRT is straightforwardly the same mode of power exercised in the use of fingerprinting since the turn of the 20th century. The goal of power then, as now, is to identify specific individuals. As the police force identifies an individual through their fingerprints, that individual can then become subject to the coercive power of the police. The agent is the police officer and/or department, and the subject are identified persons of interest. And, just as the threat of force or negative sanction is essential to operation of power in the use of AFRT, these threats are essential to the operation of power in the context of fingerprinting from the early 1900's.

The first two contexts examined in this chapter, the Church and the *cursus publicus*, are both very different contexts to the modern ones in which we can see historical continuities in the operation of power. This example is more obviously continuous with the contemporary context I am comparing it with, namely the use of AFRT by police today. It is straightforwardly evident that the key features of Dahl's account of power are present in both the context of the police use of fingerprinting technologies in the early 20th century and their use of AFRT in the early 21st century. These features, namely the presence of a social relationship where one party acts in a way that makes another act in a certain way, a definable base, means, scope and amount of power, and the presence of conflict, are all part of the way in which the police used fingerprinting technology as it was being developed. The police are the state's primary instrument of coercive power. They have the legal right to force members of the public to do things they would not voluntarily do, such as submit to arrest or investigation. The bases of police power include authority to issue fines and make arrests, public acceptance of the legitimacy of policing, and the rules of evidence that provide legal justification for action against a suspect. Fingerprint databases are a crucial component of the evidence system, and so constitute one of the bases of police power. The means of power here, as Dahl uses the word means, is the exploitation of the base of power as a mediating activity between *A* and *B*, here being the identification of the individual through fingerprints.

The way in which police use AFRT today is quite like the way in which fingerprinting was used when it was first developed, and to a large extent is still used today. As such, it is quite straightforward to see the operation of the same kind of power in the context of the police use of AFRT as in their use fingerprinting. However, there are some significant differences between the two contexts. Firstly, AFRT can operate at an increased range when compared with fingerprinting, as AFRT can track and capture faces at a distance where fingerprinting requires direct physical access to a person to capture a fingerprint. Secondly, AFRT transforms public spaces into passive spaces of surveillance in ways that fingerprinting cannot. While fingerprints can be lifted from public objects, that requires a direct intervention, while AFRT often operates autonomously and continuously within spaces. While it is important to recognise these changes, we can nevertheless see both fingerprinting and AFRT as instances of a Dahlian power, with similar or identical goals, agents, subjects, and means.

Pandemic Tracking and Plague Surveillance

Foucault describes the regulations set out in an order from Paris to control and eliminate the plague in French towns and cities at the end of the 17th century, though he notes that such orders were commonly made before this time (Foucault 1995, pp. 195-198). First, the town and its outlying districts are closed down, with inhabitants forced to remain within the town on pain of death. The town is then divided up into quarters. Each quarter is governed by an "intendant" who then appoints "syndics" to watch over individual streets. The syndic locks each house on their street from the outside, handing the keys to the intendant. Families were responsible for gathering the necessary supplies, but bread and wine were delivered regularly by wooden canals running down the street and pulley systems were constructed to deliver meat, fish and herbs. Movement on the streets was highly restricted – the intendants, syndics, and guards were the main individuals allowed outside, followed by the "crows" (who perform tasks like carrying the sick, burying the dead, and cleaning), and if absolutely necessary residents who can only leave their houses in turns.

The guards, made up of the local militia, guard the town gates and every street to prevent disorder and ensure the directions of the magistrate and intendants are followed. The syndic must daily approach each house on their street and call each inhabitant by name to appear at a window to report their health (on pain of death). The intendant then must visit the quarter they are responsible for and receive reports from syndics on both the health of the residents of each street, as well as any other important information. Then each intendant must report to the magistrate or mayor of the town, centralising the information gathered from the multi-layered surveillance system.

The magistrate has the ultimate control over the town at this point. At the start of the "lock up", the magistrate sets down the role of every inhabitant, creating a master document bearing 'the name, age, sex of everyone, notwithstanding his condition' (Foucault 1995, p. 196). Copies of this document are made and distributed to intendants and syndics to aid in their surveillance, but more importantly the master document is then continuously updated with deaths, illnesses, complaints, and any other observations. The magistrate also has control over medical treatments: they prescribe the physicians who can treat the sick and the apothecaries who can prepare medicine. They even have control over the confessors who visit the dying. The magistrate ultimately must know who moves where and when, what they are doing, and who comes into contact with others.

Then, five or six days into the lock up, houses are purified one by one. The inhabitants of a house are made to leave, their possessions suspended from the ceiling and doors, and windows sealed with wax. The house is then flooded with perfume which is set alight. Four hours after the perfume is consumed, the residents are allowed back in. Each resident would also be searched both on leaving and re-entering the house to make sure they did not carry something out or back into the house which had not been purified.

While lockdown measures in response to the spread of COVID-19 have in many ways not been as dramatic as the measures in response to the plague that Foucault describes (though in some countries they certainly came close), we can see direct parallels between these two contexts. Just as we can see similarities in the lockdown and tracking measures, we can see direct similarities in the mode of power at play. As it is today with COVID-19, the goal of power in the context of the plague was the suppression or elimination of disease, in this case the plague. The agent behind this mode of power is again the state or government, and the subjects are those who are infected and those who are not yet infected, with different controls directed at these two groups of people. The primary technique for the operation of power here is also constant surveillance of individual people, the town as a whole, and the plague itself, just as it is in the context of tracking COVID-19.

As in the previous examples, we can see the operation of the same kinds of power in the context of the 17th century plague regulations and in the context of modern pandemic tracking. The central features of Parsonian power, controlling the decisions of others within a legitimised system and the strategies of inducement and coercion are all evident in this context. The syndics, authorised by the intendants, control the movements of the town's residents, through inducement and coercion, in order to stop the spread of the plague. Power operates in a diffuse manner, and it works to train individuals to be better subjects as in Foucauldian power. The power of the magistrate is spread out across the hierarchical surveillance structure and from the architecture around them, requiring the townspeople to learn to self-regulate and spontaneously comply with rules and orders. Finally, conceptual features of Hobbesian power, i.e. the exertion of a causal force through direct threats from an instrumental source of power, are also evident in this context. The state's directives are ultimately backed by direct threats of force or execution of those who do not comply with the restrictions, acting as a causal force to prevent residents from moving around.

The operation of power has not changed significantly between the 17th century plague and the 21st century pandemic (apart from the use of the death penalty). In response to the spread of the plague, governments turned to the same kind of detailed and complicated web of power that contemporary governments have deployed in order to kerb the spread of COVID-19. The development of big data has not changed the nature of power, though it has changed the methods of surveillance and record keeping. In the 17th century, surveillance had to be conducted in person, and to ensure that residents stayed in their homes, keys had to be confiscated directly. In the current pandemic, data on the movement of people already available in phone records and public transport access cards has been repurposed for disease surveillance. Big data now allows for the movements of individuals to be tracked with great accuracy, which allows for some limited movement around cities because people can be tracked through technology with much more accuracy than ever before. This surveillance is also cheaper and allows for power to be spread out even more diffusely as it operates through the technology around us. While executions may be off the table, the threat of state force still lurks in the background, enabled by the spread of technology which can make state force more effective and easier to exert. Despite these differences, the operation of power exercised in the suppression of pandemics has been augmented by big data, but it has not had its nature fundamentally changed.

The Impact of Big Data

Through these historical examples, we can see that big data has not given rise to an entirely new kind of "data power", nor does it require us to abandon older ways of understanding power simply because of the development of a new technology. Modes of power that have been in operation for hundreds or even thousands of years are still relevant today, and big data has not made them obsolete as some writers suggest. The use of big data is simply the use of new tools and methods through which existing modes of power can be exercised.

However, big data technologies have had a range of impacts on the operation of power. Indeed, as Kirkpatrick suggests, 'Technology frees us from one set of physical constraints and sets us down in the midst of another. As such, it is involved in the mediation and reconfiguration of social power' (Kirkpatrick 2008). Big data, as another technological development, will necessarily impact on the operation of power, by eliminating old constraints and creating new ones. These changes though are not because big data is a revolutionary technology. They occur simply because big data, as a new technology, gives us new ways of doing things. This is not to say that big data is not a revolutionary technology. Indeed, in many ways big data is a huge leap forward in comparison to previous information communication technologies, and it will likely have a large impact on the operation of power. But we must not misconstrue new tools by which power is exercised as a new, hitherto unseen form of power.

To characterise the impacts of big data on power is difficult, as the term big data refers to a wide range of technologies that can be used in many ways. To present a full account of the impacts of big data on power it would be necessary to catalogue every possible way of using big data as a part of exercises of power, and such a catalogue would soon be out of date. In what follows I highlight three kinds of impacts that can be seen in the examples used in this and the previous chapter, as indicative of the type and scale of the general impacts that big data may have on power. The first of these impacts is that the use of big data can make power more efficient, by making it easier or more cost-effective to exercise power. The second is that it can increase the range of power, allowing exercises of power to take hold of subjects at a greater distance, both physically and temporally. A third impact is that big data can increase the effectiveness of power, amplifying the effects that power can produce on its subjects.

Efficiency

To say that big data makes power more efficient is to say big data allows for more power for less investment. That is, the use of big data makes it easier to exercise power in some way, such as through reducing material costs or by eliminating barriers to the operation of power. This in turn makes it easier to exercise power, as well as making modes of power accessible to agents who may not traditionally have had access to that mode of power. We can see an example of reduced material costs in the shift from the plague surveillance that Foucault describes to the big data enabled pandemic tracking. One of the key mechanisms of power in the context of plague surveillance is, of course, mass surveillance. A surveillance system based entirely on human observers is labour intensive and limited in its scope. While Foucault does not discuss the costs of plague surveillance, there is no doubt that such a program would have been expensive for the city to implement and maintain.

Big data-based surveillance is much cheaper than traditional surveillance because automation replaces human labour (Lyon 2007, p. 16). Big data-driven surveillance operates largely without human watchers. While the systems operations may still be supervised by humans, and the costs of establishing the infrastructure may be considerable, the watching performed by the system is done without the need for constant human effort, and the results are often analysed automatically before being presented. It is cheaper to utilise mobile phone data to track the movements of people than it is to send an individual to every window every day to make sure people are staying in their homes. It is also cheaper to automatically collect the data from surveillance efforts and collate that data algorithmically than it is to manually report to an intendant every day, who then must relay that report to a magistrate to be manually recorded, copied, and sent back out as daily records. The mode of power that exists in this context pursues the same goal, has the same agents, and the same subjects, but the arrival of big data alters the available techniques and methods that power can rely on, making it cheaper and easier to utilise.

There may also be physical barriers that either prevent or complicate the exercise of a mode of power. A new technology, such as big data, can reduce or entirely remove a physical barrier, or otherwise provide a way to avoid it. Aside from the costs associated with physical surveillance, there are also physical barriers when it comes to its operation. The Church, in its attempts to eliminate heresy, were hampered in its efforts by the sheer geographic area they needed to surveil. To work around these physical limitations, the formal inquisitions and mandatory confessions were only performed annually, and individual parishioners were then encouraged to perform more regular confessionals. While the Church was aiming to surveil and thus exercise power on every member of Christendom, they faced significant physical barriers meaning the power they exercised was hampered from fully reaching every subject.

Big data largely reduces or eliminates many of these physical and temporal barriers. Where the Church needed to send out inquisitors and spies in person to surveil the population and exercise power on them, the various social credit systems operating in China can ignore these physical barriers that otherwise stand in the way of exercising power. Of course, in many ways the idea of the social credit system is unthinkable without the development of big data, but it is overly simplistic to say that the development of big data has simply caused a kind of power to spring into existence. Rather, big data has merely made it more cost effective to exercise power in this way. It also provides methods for overcoming physical barriers that have otherwise limited the pursuit of the same mode of power within a new context.

Range

A new technology can also allow for power to operate at a distance from the subject of that exercise of power. We can think of power as having a kind of range or reach, typically set by the nature of the connection between the agent and subject of a mode of power. To exercise power on a subject, it is necessary to have some connection to that subject, whether that be physical proximity, an established relationship, or some other kind of connection. It is more difficult to exercise power at a distance. An agent can affect others in the hope that the intended subject will be impacted eventually, but direct exercises of power require a direct connection to the subject. As a brief note here, this is true even when we are looking at Foucauldian power. While Foucault argues that power does not come from any single source and is instead spread across relationships, operating from innumerable diffuse points, power requires that relationship to function. The nature and extent of those relationships will determine the range of power under a Foucauldian analysis.

The Roman road network and the *cursus publicus* is an example of a technology that dramatically increased the range of power. The Roman Empire was not the first empire in history to levy taxes, nor were they the first to build roads connecting major cities or settlements. But the Romans developed the first and most advanced road network of the ancient world, a road network so advanced that it lay the foundations for trade and politics for hundreds of years following the collapse of the empire. With the *cursus publicus*, the transmission of cargo and information between the Roman Senate and the far reaches of their sprawling empire was dramatically streamlined. More importantly, it allowed for decisions to be made, and power to be exercised, in Rome that affected people as far as 1,694 km away to the east in Constantinopolis and 2,081 km away to the north-west in Londinium.

Likewise, the development of AFRT has extended the range of power. Traditionally, even with fingerprinting databases, police forces could only exert power at a very close range. In order to reliably identify someone using fingerprints, a police officer and the target individual must be in close proximity at some point. For example, someone has had their fingerprints collected in person by an officer, and that officer (or a different one) later uses those fingerprints to identify them as a suspect. While the identification may be performed on fingerprints left at a crime scene without the suspect present, in order to make that identification the body of that suspect must have been physically available to the police force at some point in time. AFRT, however, overcomes this need for the physical collection of fingerprints and allows for remote identification and tracking of suspects. Through AFRT people can be identified at long distances, without them having been in direct contact with police officers before their identification. The range of power in this context is extended through the use of big data.

Effectiveness

The development of a new technology can also make power more effective, that is a new technology can make it more certain that an exercise of power is successful. Dahl is one of the few writers who explicitly considers the idea of different exercises of power as being stronger or weaker than others, and he quantifies the amount of power possessed by an agent in terms of the probability that an exercise of power will be successful in changing someone's behaviour (Dahl 1957, p. 203). The more likely it is to alter behaviour, the stronger or more effective that exercise of power is. Other writers do not follow Dahl in attempting to quantify power, but the idea of different exercises of power as being more or less effective than others in altering behaviour runs through the literature. Machiavelli for example looks at the nature of power as competing strategies, necessitating that some exercises of power will be more or less effective than others, and Foucault examines an evolution of power over time from sovereign to disciplinary power as power becomes more effective at changing specific areas of human behaviour.

The plague regulations that Foucault describes are a good example of how new technologies can make exercises of power more effective. The operation of sovereign power relies on the use of spectacles, like military parades, group rituals, and (most importantly for Foucault) public punishments like executions or torture. Through these spectacles, the sovereign displays what they are capable of, and exercises power over their subjects to change their behaviour. But the spectacle of punishment has only limited effectiveness. Firstly, it is only effective on those who witness the punishment itself. It may have some secondary effectiveness on those who hear about it after the fact, but the peak effectiveness of sovereign power is on those who witness the spectacle directly. In this way, the effectiveness of sovereign power is limited because it cannot reach every citizen, only those who see it. Secondly, it may be entirely ineffective when attempting to change human behaviour in certain ways or in certain contexts, such as around the plague. Threatening public death and torture may work to prevent some criminal behaviour, but it is not immediately obvious that it will scare whole populations into staying inside to avoid spreading a virulent plague. What is more effective in this context is the operation of a kind of disciplinary power, reliant on surveillance, which arranges people in time and space as they are trained to be idealised subjects of power.

We can see similarities within the context of attempts to track and contain the spread of the COVID-19 pandemic. The use of QR codes, the collection of geolocation data, and the use of dedicated contact tracing mobile phone apps are just, in a way, another method for tracking the population at risk of being infected with and spreading the plague or pandemic. But they are more effective than manual methods, as it can track greater populations, allow for real-time tracking of people as they move around, and makes the exercising of power more effective by enabling a more fine-grained level of surveillance.

Conclusion

There are potentially many more ways in which big data can impact the operation of power without fundamentally changing the nature of how it operates, but there is not space to discuss them here. What is clear, however, is that the development of big data does not of itself lead to a wholesale transformation of how power operates. Contemporary modes of power that utilise big data technologies show clear continuities with modes of power exercised in pre-modern times. When comparing the use of power by the Church in Medieval Europe and the Chinese government today, the Ancient Roman Empire and the contemporary corporate giant Amazon, police forces at the start of the 20th and 21st centuries, and French cities in the 17th century and governments around the world in 2020, we see direct continuities in the modes of power being exercised. These are exercises of power aimed at similar if not identical goals, with agents and subjects that play the same roles, and often overlapping technologies and means. Big data has not created these modes of power. Throughout history power has always adapted new technologies to improve its efficiency, range and effectiveness. Big data has transformed the way power is exercised in many contexts, but in the past power was also profoundly transformed by steel, alphabets, gunpowder, roads, the steam engine, telecommunications and electricity, and big data is in many ways a continuation of this gradual transformation in power.

This chapter has focused on the impacts that big data has that, while important, are not unique from a historical perspective. These impacts are made clearer through adopting a pluralistic attitude towards power, which helps us understand how a technology is used as part of the exercise of power within a given context and in turn how the key features of that technology impact on and alter the operation of power without fundamentally altering the nature of power. However, big data is driving unprecedented social transformations as it is used as a technology of power, and these changes raise important ethical problems. These problems are the focus of the following chapter.

Chapter 6

The Shift to the Data Double

The impact of big data on power can be situated within a continuous history of technology. While the bundle of technologies captured under the umbrella term of big data have had radical impacts on the efficiency, range, effectiveness, and scope of power, these impacts can be compared to the impacts of previous technologies, such as the Roman road network, the printing press, and the radio. I will argue, however, that there is an important aspect of big data's impact on the operation of power that is unprecedented. Big data technologies are increasingly used to generate predictions and to automate decision-making processes. However, algorithms, strictly speaking, cannot act directly on individuals, they use and act on data, as a kind of raw form of information (Kitchin 2014, 3). Human beings must then be represented in a kind of raw form that can be used to generate inferences and predictions. This raw form is a new kind of subject, the *data double*. Power increasingly targets data doubles and in so doing it shifts away from targeting human subjects directly. This raises significant ethical problems around how we can ensure that power is exercised accountably.

First, I will explore the inferential capabilities of big data. Big data allows us to identify correlations and patterns that would otherwise be invisible to us, and we can then use those patterns to make predictions and inferences about human behaviour with more accuracy than ever before. These predictions are then being used as part of decision-making processes, especially in those processes that are being automated using big data. The use of these predictions raises significant ethical problems for the exercising of power, which I will explore in more detail later in this chapter. In this section, I will explore ethical problems arising from the unfalsifiable nature of these predictions. As big data allows us to make predictions about human behaviour, the process of acting on these predictions, as well as merely making them, will often have an impact on the behaviour being predicted. Many of these predictions become self-fulfilling prophecies, which can be a source of injustice when such predictions inform algorithmic decision-making processes.

Second, before outlining how this leads to a shift in the operation of power, it is necessary to define what a *data double* is. A data double is a fragmentary digital representation of a person that both contains and can be used to make predictions about a person. These data doubles are representations of a person, built from fragments of data about that person, and are the vehicle through which inferences are made about that person such as predictions about their future behaviour.

Third, I argue that data doubles provide an alternative to human beings for exercises of power to target and take hold of as the subject of power. While data doubles are developed and used as proxies for the individuals they represent, power can take hold of these representations as a new kind of subject in two ways. The first is to use the data double as a way to identify human subjects to target. This is problematic when those human subjects are chosen because of errors in the inferences or predictions made through the data double. The second is a far more radical shift: in some instances, we can see power acting directly on data doubles as the subject of power. In these cases, the exercise of power is directly targeting the data double as an ethically significant entity, which means that the individual represented by that data double is affected by the operation of power as a kind of secondary effect.

Finally, I establish an important ethical problem this raises: the undermining of accountability. The targeting of data doubles by exercises of power, either as a way to identify human subjects or as subjects in and of themselves, undermines the important role that accountability plays in providing a check on the operation of power. To ensure that power is not abused, it is important that we can ensure that agents of power take accountability for their exercises of power, including by ensuring that power is exercised in transparent ways, that those who abuse power are faced with sanctions, and that any exercise of power can be explained or justified. The shift to the data double problematises these three essential elements of accountability by hiding and essentially "black boxing" the operation of power. While the shift to the data double may raise other important ethical issues, in this thesis I focus on how accountability is undermined, as this is essential for explaining how the use of big data as a technology of power can lead to violations of equality and autonomy.

Predictions

What sets big data apart from previous technologies is its immense inferential capabilities. There are of course many possible uses for the various technologies that make up big data, but many of the more valuable uses for big data are those that make predictions about human behaviour. This is true across a large number of domains. Financial institutions such as banks and credit unions utilise big data to predict the future purchasing behaviour of customers (Yeates 2017) and as a guide to marketing to those customers (Nikkei Asian Review 2016). The insurance industry uses big data to predict the likelihood any customer will need to make a claim so that policy prices can be set accordingly (O'Neil 2016, p. 166). Real estate agents employ big data analytics to predict who might be about to buy or sell a property in order to target advertising or go after clients (Chen 2015). Google sits at the forefront of big data analytics and have attempted to use the predictive capacity of big data to forecast upcoming flu strains and seasons (Lazer et al. 2014). The use of predictive data has even found its way into modern warfare. In recent years, especially under President Obama, the US utilised unmanned drone strikes across the Middle East, and the targets of these strikes were in part decided based on the algorithmic analysis of mobile phone metadata (Naughton 2016; Robbins 2016).

These predictions are made possible because big data is ideally suited to finding previously unknown and otherwise unknowable correlations in huge datasets. The huge volume of data that makes up big data, and the analytical techniques that are used as a part of big data, are ideal for finding previously undetectable patterns and correlations that human analysis may have never found. The processes of data mining, extracting or highlighting aggregates and patterns that exist within huge stockpiles of data (Sax 2016, p. 27), and machine learning, where an algorithm is designed to detect patterns that it then uses to give itself feedback and learn over time to detect new patterns (Kitchin 2014a, p. 110), are two of the many uses of big data which are ideally suited to the detection of “new” correlations.

These correlations are useful because they allow for predictions to be made about the operation of a larger system. A correlation, i.e. a quantifiable statistical relationship between two variables (Mayer-Schönberger & Cukier 2013, p. 53), can be described as either weak or strong. The stronger the correlation between two or more covariables, the more likely it is that an increase or decrease in one variable will be accompanied by an increase or decrease in the covariant. This is useful as it enables predictions concerning the operation of a system (Calude & Longo 2017, p. 598). For example, consider the role of data analysis in seismology (Degeling & Berendt 2018, p. 349). While seismologists are of course concerned about what causes earthquakes, it is also important to develop the capacity to predict when and where an earthquake is likely to occur, in order to mitigate any potential damage or injury. By collecting extensive data about past seismic activity in an area, seismologists can identify patterns in the data that can be used to predict an imminent earthquake.

However, correlation does not prove causation. It cannot be assumed that the appearance of covariance in a sample is evidence of causation. Indeed, there are many examples of correlations which we have good reason to believe are not causally linked. For example, statistical analysis tells us that the taller someone is, the better they are at repaying a loan, that people answer their phones more often when the weather is snowy, cold, or humid but they respond to emails more often when the weather is sunny and dry, and that business deals made during the new moon are on average 43% larger than those made during a full moon (Gage 2014). A theoretical scientific understanding of the world requires an understanding of the causal relationships between variables A sufficiently reliable correlation between variables, however, can be used for the purpose of making predictions even where there is no theoretical understanding of the underlying causal mechanisms.

Some authors have claimed that the rise of big data has essentially made the scientific method, as we know it, obsolete. For example, technologist like Chris Anderson claims that the traditional way of doing science, namely the construction and testing of a hypothesis to find causal relations, has been rendered largely obsolete by the development of big data (Anderson 2008). What is replacing the scientific method, according to Anderson, is the mathematical and algorithmic analysis of big data. Powerful processors that can process vast amounts of data can now reveal correlations and patterns that were previously invisible to humans, replacing the need for traditional experimental research in science. As Anderson puts it,

> *This is a world where massive amounts of data and applied mathematics replace every other tool that might be brought to bear. Out with every theory of human behavior, from linguistics to sociology. Forget taxonomy, ontology, and psychology. Who knows why people do what they do? The point is they do it, and we can track and measure it with unprecedented fidelity. With enough data, the numbers speak for themselves.* (Anderson 2008)

If Anderson is right, this is indeed the end of the scientific method as we know it. For Anderson, the development of big data marks a new epoch in our understanding of the world around us, as important (or perhaps even more so) as the development of the scientific method in the Enlightenment period.

However, it appears that Anderson's comments, at least regarding the philosophy of science, have proven to be overblown. Big data has emerged in the sciences as a valuable tool for guiding scientists on where to look, or for drawing attention to interesting correlations that trigger further investigation, but the development of big data has yet to entirely overthrow the usefulness of scientific causal analysis and theory building. An example of this is the Google Flu Trends project. In 2008, a small team at Google tried to develop an algorithm that could predict the spread of the flu. Taking a sample of the over two billion daily searches in 2007 and 2008, the analysts designed an algorithm that uncovered 45 search terms that had a strong correlation with official flu figures across the US. However, their success was short lived. The algorithm failed to predict the spread and severity of the 2009 H1N1 (Swine Flu) pandemic, and after adjustments were made the algorithm over-estimated the number of flu cases for the 2012-13 US flu season (Timmer 2014). As a result, the project was quietly decommissioned in 2015. Google has never offered an explanation as to why the algorithm under-predicted and then over-predicted the rate of the flu, nor has Google released the 45 search terms the algorithm learned to watch for. Perhaps Google's autocomplete function served to sway results, or in 2012-13 people were more alert to flu symptoms following the 2009 Swine Flu pandemic (Arthur 2014). Either way, the example of Google Flu Trends shows that big data-based predictions that might look promising in the short term may prove unreliable with time.

While the predictive power of big data may not be the death knell for science, it does however offer us the ability to make predictions in complex social systems that are difficult to explain through purely causal analysis. In the hard sciences, systems may be complex, but they can often be simplified down in reliable ways, making it easier to establish causal relations between things. In other areas, such as business, politics, law enforcement, and sociology, it is much harder to reliably simplify the complex social systems that exist in these domains. While we may still be interested in understanding cause and effect in these systems, where the complexity makes it difficult to develop a causal understanding, a correlation-based prediction may still be useful. Where having that prediction, even if there is a risk of error, offers some tangible value to a business, government, or institution, then it is often better to have and act on that prediction than not have it. Big data then offers a new and powerful tool by providing these predictions in systems that otherwise resist causal analysis because of their complexity.

The reliance on big data driven predictions becomes problematic however when we consider the often-unfalsifiable nature of the predictions that big data allows us to make. Falsifiability, as Popper (2002) proposes it, is the claim that a prediction is not guaranteed to be true; that there are possible circumstances in which the prediction could fail and thus be shown to be false based on external criteria. The idea of falsifiability is an essential part of the scientific method according to Popper, as no number of experiments or observations can ever prove a theory to be true, but one experiment or observation that contradicts a theory can and will refute it. For a prediction to be falsifiable, it must be possible to observe some external criteria or effect that would refute that prediction. If a seismologist predicts that an earthquake will happen, but the predicted earthquake never arrives, then the prediction is falsified. Although this is a failure in one sense, the prediction made a substantial claim about the world, and in that sense the prediction said something scientific. In response to such failures, the methods by which that prediction was made can be adjusted to improve future accuracy, although all scientific predictions must eventually face the same kind of test against external criteria.

In general, predictions made in the hard sciences do not themselves affect the events they describe. When a seismologist makes a prediction about any upcoming seismic activity, the prediction itself has no impact on any potential earthquake. An earthquake either will or will not happen, and the presence of a prediction about that earthquake will have no impact on it happening – the earthquake doesn't care about the existence of any predictions about itself. The presence of a prediction will impact on how much damage that earthquake may cause as it may allow for more time for people to prepare for any earthquakes, but it has no sway over the actual chance of an earthquake.

However, many of the predictions made by big data, especially those that concern human behaviour or non-natural systems, exert an influence over the realisation of those predictions. Say I predict that the shares of a given company will soon rise in value and based on that prediction I and my close friends and family purchase some of those shares. The purchase of those shares may lead to an increase in the value of those shares, and our actions based on that prediction in some way contributes to the ultimate accuracy of that prediction. For example, banks are increasingly using big data analytics to make predictions of a potential customer's likelihood of defaulting on loan or credit card repayments. For an individual categorised as a high risk of default, the denial of a loan or credit card may in fact make that person's financial situation even more precarious, thus making it more likely they will default on some other debt, which in turn worsens their credit score. Predictions about individuals may also be unfalsifiable in another sense, in that the decision makes it impossible for the subject of the prediction to prove that prediction wrong. A person unfairly denied a loan has no way of demonstrating that he or she would, in fact, have repaid the loan. These predictions about human behaviour have the very real risk of becoming self-fulfilling prophecies and, more importantly, they are essentially non-falsifiable.

Anderson's (2008) claim that big data makes causal theories obsolete misses this problem. For Popper, and others, the requirement of falsifiability is a way to keep out meaningless pseudoscience that could not be investigated. Where our aim is a scientific understanding of the causal nature of the world, unfalsifiable predictions will be regarded as meaningless, or at least treated with healthy scepticism. But big data can be used to produce new predictions, with dramatically increased accuracy, in domains which have traditionally been hard to make predictions in. The usefulness of these predictions makes them valuable, and they are now widely used in society as part of decision-making processes. Unlike traditional scientific theory, big data-based predictions do not merely describe the world but may transform the world at the same time. Big data-based analytics generates predictions which, when acted on, reduce their own falsifiability. Rather than thinking that these sorts of claims need to be rejected or removed from science (as Popper's view suggests) we need to understand how they work and how they can be used to exercise power.

These "self-fulfilling prophecies" transform the operation of power at the level of the subject of a mode of power, that is what an exercise of power takes a hold of and acts on. Power is shifted to target and act on what I refer to as "data doubles" rather than directly on human subjects. As predictions are made and relied upon, power focuses on manipulating or controlling data doubles as a means of acting on individuals or groups. Before discussing how data doubles are targeted by power as its subject, it is first necessary to outline what a data double is.

The Data Double

Artificial digital profiles are becoming the central subject of power, displacing those individuals who have traditionally been the subject of social power. But what is the data double? Haggerty and Ericson (2000) proposed the idea of a data double as a kind of informational doppelgänger, a new body constructed through surveillance:

> *Culled from the tentacles of the surveillant assemblage, this new body is our 'data double', a double which involves 'the multiplication of the individual, the constitution of an additional self' (Poster 1990: 97). Data doubles circulate in a host of different centres of calculation and serve as markers for access to resources, services and power in ways which are often unknown to its referent. They are also increasingly the objects toward which governmental and marketing practices are directed (Turow 1997). And while such doubles ostensibly refer back to particular individuals, they transcend a purely representational idiom. Rather than being accurate or inaccurate portrayals of real individuals, they are a form of pragmatics: differentiated according to how useful they are in allowing institutions to make discriminations among populations. Hence, while the surveillant assemblage is directed toward a particular cyborg flesh/technology amalgamation, it is productive of a new type of individual, one comprised of pure information.* (Haggerty & Ericson 2000, pp. 613-614)

The data double, as Haggerty and Ericson and other writers (Lyon 2007; Matzner 2017) describe it, is a digital profile of an individual. This profile is constructed from fragments of personal data collected through surveillance, which 'can be rather freely used, compared, transferred, and processed, creating new distinctions, groups, values, and needs for action.' (Matzner 2017, p. 31). They are used as reference points for individuals, a way to identify, categorise and mark them.

In defining the data double, Haggerty and Ericson draw on Deleuze's and Guattari's work on surveillance. As a result, the concept of the data double is, in some respects, derived from Deleuze's concept of the "dividual" (Kubler 2017, p. 7). The dividual is the result of the operation of control on an individual (Deleuze 1992, p. 5). Deleuze's concept of 'control' describes a form of power that operates through a process of modulation. Deleuze describes the idea of modulation as 'like a self-deforming cast that will continuously change from one moment to the other, or like a sieve whose mesh will transmute from point to point.' (Deleuze 1992, p. 4). As an individual is subjected to control, they are acted upon by a continuous force that shapes them over time, and as they are changed over time, they are divided into many varying dividuals. These dividuals are a kind of sample of an individual, a fraction of the person that can be used by the operation of power, and in this way both the dividual and the data double are useful proxies for individuals. So, where Foucauldian discipline would subjectivise an individual as a patient in a clinic, for example, Deleuzian control would instead divide the individual into a dividual by taking the information that is relevant to the operation of power at that time (such as vital statistics, needs, and medical history) to create a profile of that person. As power as exercised, the individual is divided again and again in different ways, creating more dividuals to make future exercises of power more effective.

Additionally, dividuals and data doubles are both more flexible and malleable than the individual they originate from or relate to. The divisions made in the individual and the data used from the individual to create the data double are easy to manipulate and change based on who is making the divide or creating the double, making both the dividual and data double easy to use and change at will. But there is a key difference between the two. The dividual is a part of a larger individual, while a data double is a creation above and beyond an individual. The dividual is created within the individual, by acting on the individual and their body. No matter how fine the divisions or how many divisions are made, they are all still a part of the individual. The data double on the other hand exists outside of the individual. The data double is created from collected data and exists outside of the body. It is not produced through division, but through compilation.

While Haggerty and Ericson's account of the data double is widely used in the literature, there are other concepts with similar content. Amoore (2011) proposes the "data derivative", which functions similarly to the data double but takes a stronger influence from financial derivatives. The data derivative as Amoore describes it is a construct inferred from fragmented elements of data that can be traded, shared, or exchanged separately from those fragments of data that make it up (Amoore 2011, p. 28). Importantly, data derivatives do not need to be constructed from an individual's personal information and can be built instead from collected data fragments from any source. Cheney-Lippold (2011) uses the term "algorithmic identities" and focuses on how the algorithmic infrastructure of the internet classifies and identifies individuals to create what this algorithmic identity. Crucially, although this algorithmic identity is beyond the control of the individual in question, it is an inseparable part of that person. Finally, Burkell (2016) refers to an individual's "digital shadow", a detailed and deeply informative record created with a combination of user-generated data (digital footprints) and data generated about a user by others (data shadows) that ultimately can come to stand in for that individual and their identity when interacting with digital systems and decision-making processes. I will be using the term "data double", but I will define the concept differently from the definition proposed by Haggerty and Ericson.

In this thesis, the term "data double" will be used to refer to a fragmentary digital representation of a person that both contains and can be used to make predictions about that person. There are several elements to this definition. First, data doubles are fragmentary in nature. This is because data doubles are largely used in a specific domain or for a specific purpose and will thus only contain data about an individual that is relevant to that domain or purpose. So, a data double that has been constructed by a bank or financial institution for the purposes of analysing loan applications will contain data about an individual's financial history, but may not include their browser history, while a data double built for the purpose of targeting advertising will contain different categories of data. In this way, a data double is not a full reflection of an individual, nor is it a new kind of "informational self" as Haggerty and Ericson suggest it might be. They are only fragmentary. As a result, an individual will not have one data double, rather they will have many data doubles representing different aspects of them. The same bits of data about an individual may be used in multiple data doubles, meaning that any given individual can have an unlimited variety of data doubles constructed around them.

As data doubles are fragmentary by nature we should think of a data double as a constructed, and often partial, representation, as fragments of data are used to build a data double that represents and individual in a specific way, rather than reflecting the individual as a whole. This is largely because data doubles are created for a purpose. Data doubles are created through the deliberate, though often automated, collection and analysis of data. The reason why a double is created, the purpose it will be used for, will both determine the data that goes into making the double and how it is constructed, i.e. how the person will be represented by that double.

We must also not think about a data double as a high-resolution representation of an individual. They are an approximation – the data that goes into a double is widely variable at best, often inaccurate, and never comprehensive. Additionally, while many data doubles will be drawn from a single person, there will be occasions where the data used to construct a double does not come from a single person. It is possible to have a data double of a group of individuals, either accidentally or deliberately. For instance, where individuals share access to a digital platform, like a family computer or online account, then data collected from different users may be falsely attributed to a single data double, or alternatively a double may be deliberately constructed of a group of individuals. It is also possible to have a data double of a non-human. In 2018, "bots" (automated programs such as those used by travel sites to trawl for flight prices or those used to perform denial-of-service attacks) accounted for 37.9% of all internet traffic, down from previous years where over half of all internet traffic came from bots (Hughes 2019). As these bots function, especially on social media platforms, other automated processes may collect data about their activities and build a data double, incorrectly seeing that bot as a real person. While data doubles may allow for novel representations of an individual, using data that has never been able to be collected before, they are still only sketches, and sometimes very crude ones at that.

Another important aspect of data doubles is that they are "predictive"; they contain and enable predictions about the individual they represent. There are two senses in which a data double is predictive. The first is that they are can be used for predicting the future actions of the individuals they represent. By collecting and collating data on a person's past behaviour, the data double can reveal patterns about that person which in turn can be used to predict future behaviour. For example, a data double may be constructed using geolocation data from a mobile phone, and an analysis of that data double may lead to the prediction that, based on past movements, they will shop for groceries at a certain location at a certain time. The second sense in which data doubles are predictive is that data doubles may be used to make inferences about characteristics of a person from apparently unrelated data. For example, a person's gender, political views, or psychological traits may be inferred from the pattern of "likes" that person posts to Facebook pages (Kosinski et al. 2013). These inferences are then incorporated into that data double, or are used to generate a new data double, which can in turn be used to make further predictions or inferences about that person.

A fourth key feature of data doubles is that the person represented by a data double will usually have little or no influence over the construction of a data double. This is for two reasons, the first being that data doubles are often largely invisible to the person they represent. Data doubles will often be constructed and stored in databases that are inaccessible to the person they represent, and their use in decision-making processes is almost always performed out of the view of the person that double represents. As such, it is often difficult for someone to know if a data double has been constructed and used as part of an algorithmically driven decision-making process. The second reason is that data doubles are often created from data owned by a corporation or government institution, and usually through algorithmic processes that are also owned and controlled by corporations or government institutions. While a person represented by a data double will have some indirect influence over "their" data double, such as by deliberately providing data or challenging the accuracy of any data that has been collected, this influence is very limited. Those who control the data used in the creation of a data double, and the processes through which those data doubles are created, are the ones who ultimately have control over how people are represented by "their" data doubles.

Finally, a data double is designed for a purpose. There are two general uses for data doubles. The first is to categorise the individual it refers to as belonging to a group or category, and the second is to make predictions about a person's future behaviour. The types of data used in constructing a data double are determined by the purpose it is used for. For example, banks rank potential loan applicants based on an assessment of the probability the applicant will default on future loan repayments. A data double constructed for this purpose will include financial data such as past and current debts, credit card purchasing history, currently owned assets, employment history, place of residence, average salary in that neighbourhood, and more (Precious 2020). This data may be irrelevant for a data double in a different context, such as where a university is looking to differentiate between students based on predictions of academic success.

A data double, however, is not just a way to identify and differentiate between individuals. It can also stand in for them. For Haggerty and Ericson (2000), the primary use of data doubles is for discriminating between individuals. They provide an easy way to label and differentiate individuals based on the relevant purpose. Haggerty and Ericson, and others, use the word "double" in the sense of a representation. But there is another sense of the word "double", and that is to stand in as a replacement. By this I don't mean a perfect replacement, like a doppelgänger of a person. This is not the case, because data doubles are essentially fragmentary in nature. Instead, I am using it in the sense of a stunt double. Like a stunt double standing in for an actor, the data double only needs to be good enough for the desired purpose. It is not necessary for a stunt double to be identical to the actor they are standing in for. All that is needed is that they have a matching haircut, a similar height and build, skin tone, wardrobe, or maybe even the same nose. So long the resemblance is adequate, the stunt double is able to substitute for the actor they are standing in for, such that the audience is unaware of the substitution. Likewise, it is only necessary that a data double bears enough of a resemblance to an individual, through a matching IP address, shared geolocation data, snippets of a browser history, or other data, that it can stand in for them as needed.

In many ways data doubles are not a new phenomenon. Ever since records have been kept, data doubles have been in existence, and “small data” databases contain and give rise to data doubles that can and have been used to make inferences and predictions about people. Indeed, much human research is built on the construction and use of data doubles as representations of people, and any time data is collected about an individual it can be used to create data doubles. What is important here is a difference in scale. Big data technologies, particularly AI and machine learning, can create and utilise data doubles faster than ever before and with finer grained detail than ever before. The data doubles that can be created from a small database, even where it is digitised, often require manual construction and/or interpretation, and will draw on only a select amount of data which is usually carefully curated during the collection process. Big data technologies mean that data doubles can now be made with more data, and thus more granularity and detail, and can be created and transformed automatically by algorithmic processes.

Power and the Data Double

Having explained what the data double is, it is now necessary to set out how they can be used by power to affect the individuals they represent. Exercises of the kinds of social power we are interested in here have traditionally targeted human subjects. That is, in order to pursue its goal, an exercise of power takes hold of and acts on a person or a group of people as its subject. For example, Foucauldian power takes a hold of the body of a subject. By surveilling and controlling the position of the body, over time the subject internalises the operation of power through self-regulation. In contrast, Parsonian power looks to take hold of the subject through control over their decision making. A successful operation of one of the four strategies of power results in the human subject of power changing their behaviour by essentially ceding their decision making to the agent of power. All three dimensions of Lukian power takes hold of a subject through their interests. That is, power operates by altering the interests of an individual directly, indirectly, or by negating them. While the various accounts of power vary in how power takes a hold of the subject of power, they each function by taking a hold of a person or a group as the subject of power. By targeting a person’s body, sense of obligation, or interests, each account of power is taking hold of the person directly as the direct subject of power.

While data doubles may have initially been conceived of as a way to categorise or differentiate individuals, they are increasingly becoming the target of power directly, even to the point of supplanting humans as the direct targets of power. Where power has traditionally taken hold of people, such as through their body, sense of obligations, or interests, power can now take hold of this new digital entity as its subject but still affect the people those digital entities represent. In claiming that the data double becomes the subject of power or that power can now act on a data double as the “direct” subject, I am not claiming that data doubles are in some sense moral patients or that they have interests that are impacted by the exercise of power. Indeed, it is always ultimately a human who is being impacted by the exercise of power even where a data double is the subject of that exercise of power. Data doubles are subjects of power in the sense that they are entities being manipulated by the exercise of power. That is, that exercises of power are tailored or modulated according to a data double, and the person that data double represents is then indirectly manipulated in a novel and ethically important way.

This is not to minimise the importance of analysis of algorithms as black-boxes, nor their role as a key mechanism through which power can be exercised. But there is something missed if we focus only on the algorithm. We need to consider how the decisions made by the algorithm, or with the aid of an algorithm, can then impact on individuals, and I argue that this is because exercises of power can use algorithms to operate on data doubles in the same way that we are familiar with more "traditional" exercises of power operating on individual's bodies or interests.

Importantly, there are two senses in which the data double "becomes" the subject of power. The first is where power is still ultimately concerned with human subjects but data doubles are used to take hold of those human subjects. The second is where power becomes disinterested with persons, and the subjects of power (the entities that power is looking to affect) are data doubles directly.

In contexts where we can see the first sense of this shift to the data double, the exercise of power is still ultimately concerned with humans as subjects. However, the proliferation of data doubles means that power has new ways of identifying and taking hold of those persons it is targeting as subjects. Big data has given rise to this new digital entity which can be used as either a kind of proxy for a person or to identify specific individuals to target with exercises of power. In this sense, the data double acts as a representation of an individual in decision-making processes that are assisted or made by algorithms. In a way this sense of a shift in power is close to the initial usefulness of data doubles, i.e. as a tool for identifying or predicting individuals who would then be subjected to an exercise of power.

This shift in the way power is exercised is, in a way, the result of the actuarial potential of data doubles. The predictions that can be made using data doubles are ideal for the operation of actuarial science, where statistical methods are used to assess risks within a system. While traditionally actuaries have primarily operated in the financial and business world, assessing the potential risks and benefits of investments and other opportunities, there is a growing trend of using actuarial methods in other systems, notably in criminal justice (Silver & Chow-Martin 2002). Actuarial methods will also likely prove useful in any system that is concerned with the risk of disruption or loss based on the actions of individuals within that system.

These predictions can then be seized upon as part of the exercise of power in two ways. First, as a justification for an exercise of power. If a data double is used to predict or contains a prediction that an individual poses a risk of disruption, that becomes a prima facie reason for the exercise of power to prevent that disruption. If anyone were to ask why power was exercised in that context, the answer could and would be given that power was exercised because a model using a particular data double predicted that the individual corresponding to that data double poses a risk to the stability of the system. Second, these predictions are a guide for the operation of power.

Depending on the prediction, e.g. the probability of the disruption, or the nature of the potential disruption, power will be exercised in different ways. If, for example, an individual is predicted to pose a risk by committing a violent crime for example, then power can be operated to keep that individual under surveillance or restrict their access to potential weapons. The subject will be directly targeted by the operation of power, but how that power functions will be at least in part dictated by the risk predicted by the data double.

The second sense of the shift in power is where exercises of power target data doubles as the primary subject of power, rather than as a proxy for an individual or a way to identify an individual. This is a more radical shift in the way in which power can be exercised. As discussed above, power has traditionally operated on human subjects. But the development of big data and the subsequent rise of data doubles is facilitating a shift in how power is exercised. In this second sense, power is acting not on a human subject, but on a data double as the primary subject of power. Power is taking as its primary subject the increasingly important data doubles, which have become valuable abstract entities in their own rights. The individuals represented by these data doubles, who would traditionally be the primary subjects of power, will now feel the impact of power operating on those data doubles, but only as a kind of side effect. This is not to say that any agent who is exercising power is only thinking of data doubles. It is likely that an agent will still intend for a human to be impacted by their exercise of power. But that human is no longer the direct subject of power.

We can say that data doubles become the subjects of power in this sense based on how they are used as part of algorithmic analysis. As algorithmic outputs are used to generate decisions or actions, the inputs used in those algorithms, such as data doubles, are essentially treated as being facts. So far as the exercise of power is concerned, the data double is reality, in the sense that it becomes unimportant whether the data double is an accurate representation of some person. If a data double is ineligible for a loan, then the person it represents is ineligible for a loan. If a data double is assigned a poor social credit score, then a person is thereby socially discredited. Data doubles are the raw material for algorithmically generated predictions that then become social facts in the world.

Algorithmic analysis is not performed on people, it is performed on data doubles, which are limited and partial representations of people. When someone's activity on the internet is analysed, it is not the individual as a whole who is analysed, rather a fragmentary set of data points derived from their browsing history constitutes the raw material for analysis. What comes to matter, from the point of view of power, is whether the data is the *right* data, not whether that data *is* right, in that it accurately represents some external reality. This is in contrast to the first sense of a shift towards data doubles as subjects, where the data double stands in as a kind of proxy to identify a person as the subject of power. In this second sense, the decisions that are made and any exercises of power undertaken are made and done based on the reality that is represented by the data double, and is thus directed at the data double rather than any individual that data double represents.

As power is then exercised on data doubles, and those doubles are manipulated or controlled, the individuals represented by those doubles will still feel the impact of power. As the social facts of the world are altered in response to the exercising of power on the data double, individuals represented by those data doubles will have their choices and behaviours limited by the changing world around them. There are a number of reasons as to why individuals will have their behaviours limited, including through the operation of direct coercion as in the case of the Chinese credit score systems (if you have a low score, you cannot travel), but in many cases individuals will be “nudged” to behave in certain ways.

A nudge may be defined as ‘any aspect of the choice architecture that alters people’s behavior in a predictable way without forbidding any options or significantly changing their economic incentives.’ (Thaler & Sunstein 2008, p. 6). The example that Thaler and Sunstein provide is the arrangement of food on the shelf at a shop. Banning unhealthy foods is a form of coercion but placing healthy food like fruit at eye level is a nudge. It is an arrangement of the space, the “choice architecture” around an individual to guide them to make specific choices without forbidding them from making others. As data doubles are manipulated by power they can be (and often are) used to construct a choice architecture around the individual they represent based on the predictions they make about them. For example, if a data double predicts an individual will be more likely to purchase an item if they are shown a specific form of advertisement at a specific time, then power can be exerted on them through showing them that form of advertisement, essentially building a kind of choice architecture around them.

The Ethical Problem of the Data Double

The shift to the data double, in both senses, raises important ethical issues concerning the operation of power. In short, big data undermines accountability. Accountability is an important check on the operation of power: it works to both prevent and redress abuses of power, as well as to provide avenues for challenging and appealing decisions. Accountability subjects power, or those exercising it, to the threat of sanctions, it requires that power be exercised in transparent ways, and it forces those exercising power to explain their decisions and actions. In other words, accountability has aspects of enforcement, monitoring, and justification (Schedler 1999, p. 14). When we say that someone or something is accountable for their actions, we mean to say that that person or institution should take responsibility for their actions, that they should be able to provide an explanation of their actions, and that there are penalties for negligence of malfeasance. However, the use of big data, and in particular data doubles, undermines accountability, in two ways: by making it easier for those exercising power to avoid responsibility for their decisions, and by making it harder to determine whether those decisions were sound. These problems of accountability arise for three reasons. First, as power relies on unfalsifiable predictions it becomes difficult to assess the accuracy of power. Second, the operation of power gains a veneer of objectivity that makes it difficult or impossible to challenge. Third, decision-making processes are black-boxed, effectively excluding both subjects and agents of power from understanding how power operates.

First, the shift to the data double makes it difficult to evaluate decisions. Data doubles are predictive, in that they contain inferences and enable predictions about the individuals they represent. As discussed above, many of these predictions are unfalsifiable, and as a result we cannot easily assess whether these predictions are accurate. In turn, it is difficult to monitor and evaluate exercises of power that rely on or utilise these kinds of predictions. As we cannot evaluate the accuracy of the predictions that form the basis of an exercise of power, in turn we cannot easily monitor the appropriateness of that exercise of power. Indeed, in many cases, it will be the exercise of power which make an unfalsifiable prediction "come true". In these cases, it is not just that power is difficult to monitor, but that the exercising of power itself is what makes it difficult to monitor, directly undermining accountability.

Furthermore, it becomes difficult to monitor the operation of power insofar as it becomes difficult to see who will be affected by an exercise of power. When using data doubles, the wielder of power can, in a sense, pre-define the subjects they are looking to act upon in a highly precise manner. For example, an agent can look to exercise power on single men between the ages of 20 and 30 who live in two-bedroom apartments in Sydney, Australia and own a cat. Then, the algorithmic system that that agent is using will assess the various data doubles it has access to, find those data doubles which fit those parameters, and those individuals whose doubles contain or infer those characteristics will be affected by operations performed on those doubles. But, while agents of power can be incredibly precise in their selection of data doubles, they are essentially blind to which individuals will be impacted by the operation power. They are wielding power to affect a set of data doubles that match pre-selected criteria, and usually do not know which individuals in the world will be impacted by that exercise of power. This ignorance as to who is being targeted is exacerbated in cases where machine learning selects the data doubles.

Second, the use of data doubles means that it is difficult to challenge exercises of power and threaten agents with sanctions for any abuses of power. This problem arises because power acquires a veneer of objectivity, making it seem as if any decisions made or influence exerted are based solely on objective facts, and are therefore not open to questioning. There have always been errors, or abuses, in the exercise of power and subsequent issues of fairness and justice. An important example here concerns the history of racial bias in sentencing, parole, and bail decisions across many jurisdictions, including the US and Australia. Proponents of big data-based approaches to these decisions have claimed that they can be used to replace subjective, biased, and imprecise decision making with an objective, unbiased, and precise approach. Advocates of using big data for legal decisions claim that automated methods are not subject to human biases and error:

> *For more than two centuries, the key decisions in the legal process, from pretrial release to sentencing to parole, have been in the hands of human beings guided by their instincts and personal biases. If computers could accurately predict which defendants were likely to commit new crimes, the criminal justice system could be fairer and more selective about who is incarcerated and for how long.* (Angwin et al. 2016)

These approaches are often driven by a belief in the objectivity of data (Mittelstadt & Floridi 2016; van Dijck 2014), and they have become highly influential.

Despite these promises, we have yet to develop an AI that capable of consistently accurate predictions. While big data may be offered as a way to avoid human biases and error, the data driven tools we are using still contain error rates themselves, and as such the exercises of power that use these tools still operate with the risk of error within them. But now these errors are hidden behind a veneer of objectivity, based on a belief that because we are making decisions based on cold, mathematical analysis of hard data then our decisions and exercises of power are similarly objective. By promoting the analysis of data as objective and free from bias, a kind of mythology can be built up around it, hiding biases and errors behind this veneer. Once hidden, it becomes difficult to find them, or even find where to look for them. If we cannot find these errors, if we cannot notice abuses of power behind the veneer of objectivity, we cannot then enforce sanctions aimed at errors and abuses, which removes the teeth of accountability.

Finally, and perhaps most importantly, the use of big data brings up a major problem when it comes to justification, in that the operation of power becomes black-boxed and unable to be justified. As power acts on data doubles as a subject, in both senses, power becomes opaque to those individuals who are impacted by power. In effect, power becomes black-boxed. The mechanisms or means by which power functions become harder to see, both for those being affected by the operation of power and by those exercising power. At best we can see the end effects (assuming we can correctly identify those affected by it), but the way the subjects of power are affected becomes hidden from view. How the use of data doubles makes it difficult to justify power differs between the two different senses of the shift to the data double.

For those modes of power where power uses data doubles to identify and then act on people, power is mediated by data doubles. Where power is still acting directly on people as its subjects, it is more obvious that they are being affected by an exercise of power. But the use of the data double to identify them may make it hard for them to determine how or why they are being targeted by an exercise of power. This means that it will be difficult, or in some cases impossible, to provide a justification as to why an individual is affected by an exercise of power. Of course, we can probably say that power has been exercised here because of the predictions of the data double, but that is not a particularly satisfying justification. What are these predictions, how and why were they made, and perhaps more importantly, why are they the basis of an exercise of power? These and other questions are difficult or impossible to answer as a result of the use of data doubles to identify subjects.

In those cases where power acts on data doubles as the subject of power directly, it can become opaque, or at worst entirely invisible, to the individuals represented by those data doubles. This opacity is largely a result of the way in which power nudges individuals. The essential nature of a nudge is that it is subtle, it is designed to influence a person's choices without alerting them to that influence. A shopper is not being told to eat healthy but having fruit at eye level subtly influences them to lean towards that purchase. Likewise, an individual is not told to act a certain way, such as click on an advertisement or vote a certain way, but they are being subtly nudged to do so based on the choice architecture built around them. While power becomes hard to justify where data doubles are merely used to identify subjects, where data doubles become the subjects themselves it is even harder to justify, especially where those individuals being impacted by it are unaware of the operation of power around them.

The shift to the data double does not just make power opaque to those individuals who are the subject (or the collateral damage) of an exercise of power. It also makes power opaque from the perspective of any agent exercising power. While an agent of power will likely be aware that they are exercising power in some way, the use of data doubles as either a way to identify a subject, or as the subject directly, makes the operation of power opaque to agents as well. This opacity in the operation of power arises from the opacity of machine learning algorithms due to intentional corporate or state secrecy, the technical illiteracy of users and "subjects", and the characteristics of machine learning and the scale they operate at (Burrell 2016). Where big data is used in the exercise of power, this opacity arises both in the automated creation and transformation of data doubles and in the automation of decision-making and targeting of data doubles with the exercise of power, and this opacity arises both for those individuals impacted by the exercise of power and for those who exercise power. Even in situations where a justification may be demanded and the relevant agents want to give that justification, the agent of power and those around them may not be able to offer a justification because they themselves cannot discover it. Power becomes opaque to those affected by it and to those who wield it, and in the worst cases makes it impossible to justify or explain.

The undermining of accountability through increased difficulty in evaluating exercises of power, imposing sanctions for abuses of power, and justifying exercises of power, are an important part of how the use of big data in the exercises of power can lead to unfair discrimination and the limiting or undermining of autonomy. While there are likely other important ethical problems that arise from the use of big data as a technology of power, the undermining of accountability is an important problem that can result in the violation of norms of equality and autonomy. How these may be violated will be explored in more detail in the following chapter.

Conclusion

I argue that an important effect of big data as a technology of power is that power begins to act on the inferences and predictions generated through the use of big data. This shifts social power away from targeting people as the direct subject and towards targeting data doubles as the subject of social power. Data doubles, representations of individuals made up of fragments of data about those individuals, become the subject of power in two senses. First, the data double mediates the operation of power. Some exercises of power use data doubles as proxies to identify human subjects to then target as the subject of power. Second, power is exercised directly on the data double, in which case the data double becomes the subject of power in and of itself, and the individual it represents is impacted as a kind of side effect.

Ultimately, this leads to a major ethical problem with the exercise of power, whereby accountability is undermined. The use of big data and the targeting of data doubles as the subject of power limits our ability to enforce sanctions to punish abuses of power, makes it difficult to monitor the operation of power by drastically reducing the transparency of exercises of power, and makes it difficult if not impossible to provide justification or an explanation for why power has been exercised. These are significant ethical problems, and by grasping these problems we can understand how the use of big data in decision-making processes can and does lead to the harms discussed at the beginning of this thesis, i.e. unfair discrimination and the undermining of autonomy. In the next chapter, I will look at a further four examples of the use of big data in the exercise of power to identify the relevant modes of power in each context. This will include an analysis of the continuities present in that mode of power, as well as an exploration of how the subject of power is shifted from humans to data doubles, and how that leads to the undermining of accountability in exercises of power.

Chapter 7

Modes of Power and the Data Double

The purpose of this chapter is to bring together the above discussions on modes of power and discussions of big data leading to a shift in power towards targeting data doubles. In this chapter, I will take four further example contexts and set out their key contextual features, with which we can identify the relevant conceptual features of power present in each example. Then, by looking at the historical continuities in the operation of power before and after the development of big data, we can see the impacts that big data has on power, including increases in efficiency, range, and effectiveness as well as how power shifts towards targeting data doubles. By drawing out these impacts, we can better appreciate how power changes as a result of the use of big data in each context, and how accountability is undermined in ways that lead to ethical harms such as unfair discrimination and the undermining of autonomy. Importantly, the first two examples in this chapter focus on unfair discrimination, and the third and fourth examples show how big data can be used to undermine autonomy.

The first case is the use of algorithmic risk assessment tools in US courts during criminal sentencing and pre-trial bail hearings. These tools use big data driven analysis to assign a risk score to defendants that predict the likelihood that they will commit further crimes, either while awaiting trial or following a conviction. These risk scores are then used to guide judicial decisions on bail and the length and nature of sentences. In this context, by picking out the goal, agents, subjects, and means of power we can see key features of Weber's and Foucault's account of power. Power here is then transformed by the use of big data as it becomes more efficient and effective, but more importantly as the subject shifts to the data double power becomes black-boxed and the importance of information to power in this context is changed. This ultimately impacts on how we can ensure that power is exercised accountably, firstly because it is not possible to assess the validity of the scores, secondly power becomes harder to challenge because of its reliance on apparently objective data, and thirdly a black-box process for generating decisions makes it difficult to evaluate or criticise those decisions. Understanding how this shift in power impacts on accountability is important for contextualising unfair discrimination through the use of algorithmic risk assessments.

The second case study is the use of predictive policing technologies and techniques. Police forces across the world, and particularly in the US, are using big data to predict the likelihood that a given individual will commit or be the victim of criminal activity and the likelihood that criminal activity will occur in a certain geographical area. Police power is complex and in its various aspects exhibits elements of all the modes of power discussed. For the purpose of this discussion I want to focus on the implications of predictive policing from a Dahlian perspective. Dahl's discussion of police power pays particular attention to the social relationships and understandings that facilitate the exercise of police power. However, as the relationship between the police and the policed is increasingly mediated by databases and algorithms, the basis of legitimate police power is threatened, and as this basis is threatened the risk of unfair discrimination increases.

The third example is the use of targeted advertising in politics. In recent years, political campaigns have begun utilising targeted advertising: advertisements that are tailored for specific kinds of people, at individuals rather than at the broader voting public. To target these advertisements, psychometric profiles are created that are used to predict how individuals will behave and what will prompt them to then change that behaviour. Here we can see clearly the features of Machiavellian power, the operation of which is also altered by the use of big data in this context. Here, the use of big data makes power significantly more efficient and effective, as well as increases its range, but the shift to the data double also takes the threats and promises made as part of a Machiavellian strategy and "aims" them at data doubles rather than directly at human subjects. That is, the mechanisms of power in this context are tailored towards data doubles rather than at persons, changing the operation of power and undermining the autonomy of the subjects of power.

Finally, the fourth example is the rise of the smart city. Increasingly, city leaders and planners worldwide are turning to big data for tools to manage and optimise the operations of the city. By monitoring and collecting constant streams of data from residents' devices and vehicles, as well as environmental sensors, the city can be micromanaged in real time. In this context, we see a complex combination of features of Foucault's, Hobbes', and Lukes' accounts of power. The use of big data in this context makes power more efficient and effective and shifts the way in which people are ultimately shaped by power through nudging rather than by coercive training, thereby undermining individual autonomy.

Criminal Risk Assessment

The development of big data has led to a substantial increase in the use of evidence-based practices in the criminal justice system (Stevenson 2018), particularly in the form of risk assessment tools. Risk assessment tools have been used by the courts since the 1920's, although their use has expanded considerably in recent years. At their simplest, risk assessment tools take a set of inputs and assign points or values to those inputs. From these points or values a risk score is calculated, either manually by a human, by a conventional software program, or through a machine learning derived algorithm (Stevenson 2018, p. 315-316). Our primary concern here is with those risk assessment tools that rely on machine learning as part of the calculation of the score, but there are also risk assessment tools that utilise big data to derive the initial data inputs.

An example of the latter is the Public Safety Assessment (PSA) tool (DeMichele et al. 2020, p. 414), created using a database of over 1.5 million cases from across the US. The PSA was designed for use during pretrial bail hearings to guide judges on bail decisions. Bail will be refused where there is a significant chance that the defendant will fail to appear at trial or will commit further crimes while waiting for trial. The PSA works by predicting the likelihood of three pretrial outcomes, namely the likelihood of either a Failure to Appear (FTA) at trial, a defendant having a New Criminal Arrest (NCA) while on bail, or a New Violent Criminal Arrest (NVCA) while on bail. From the collected data, the developers of the PSA settled on nine factors to rely on when assigning a score to indicate the likelihood of an FTA, NCA, or NVCA outcome (APPR 2020):

Factor	FTA	NCA	NVCA
1. Age at current arrest		X	
2. Current violent offense			X
2A. Current violent offense and 20 years old or younger			X
3. Pending charge at the time of the arrest	X	X	X
4. Prior misdemeanour conviction		X	
5. Prior felony conviction		X	
5A. Prior conviction (misdemeanour or felony)	X		X
6. Prior violent conviction		X	X
7. Prior failure to appear in the past 2 years	X	X	
8. Prior failure to appear older than 2 years	X		
9. Prior sentence to incarceration		X	

The final risk score is calculated as the sum of the component scores for each factor. For example, to determine a defendant's FTA risk score, the defendant must answer four questions: did they have a pending charge at the time of their arrest, do they have a prior conviction, have they failed to appear in court in the last 2 years, and have they failed to appear in court more than 2 years ago. The defendant's answers will be scored, and then the total is converted to a scaled FTA risk score. A different combination of factors may produce the same risk score. The defendant may have a pending charge at the time of arrest (1 point), a prior conviction (1 point), and a prior failure to appear three years ago (1 point) or they may have one prior failure to appear within the last two years (2 points) and a prior conviction (1 point). In both cases the defendant receives the same risk score of 4. The method for calculating FTA, NCA, and NVCA risk scores is publicly available online, including the weighted points assigned to each input and the formula to convert those points into the risk score.

Significantly, the developers of the PSA have avoided using demographic information other than the age of the defendant (and even that is a simple binary question of whether they are younger or older than 23). All the inputs used can also be readily obtained from administrative records. This both increases the simplicity of the system, and according to developers reduces the risk of predictive bias for the poor and for communities of colour (DeMichele et al. 2020, p. 414). However, as will be explained below, simply removing or avoiding obvious demographic categories does not eliminate bias from the process of establishing risk scores.

Risk assessment tools that utilise big data and machine learning for the calculation of the risk scores themselves are commonly used during sentencing. One such algorithm is COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), a proprietary risk assessment tool developed by Northpointe Inc. Defendants answer a questionnaire containing 137 questions, and should they choose not to respond then many of the answers can be obtained from criminal records. Questions include “Was one of your parents ever sent to jail or prison?”, “How many of your friends/acquaintances are taking drugs illegally?”, and “How often did you get in fights while at school?”, as well as questions presenting statements for the defendant to agree or disagree with such as “A hungry person has a right to steal” (Angwin et al. 2016). The answers given by the individual to that questionnaire are then compared to a dataset of the local criminal population, including recidivism rates, comparing the answers the individual gave to others in the area.[5] Based on the comparison the defendant is assigned a score from 1 to 10, indicating the likelihood they will reoffend in the future. Judges may use the score as part of their decision making when handing down sentences. COMPAS and other algorithmic sentencing programs are currently used across much of the US, where appellate courts have largely ruled that the risk scores are an admissible consideration when sentencing, though they should not be the only consideration used to determine sentencing (Smith 2016).

COMPAS, and other similar algorithms, have been the subject of justifiable concern. In particular, there is evidence to suggest that these algorithms are not as reliable as is claimed. An investigation by ProPublica (Angwin et al. 2016) indicated that only 20% of individuals predicted to reoffend and commit a violent crime went on to do so, but when taking all crimes into account including misdemeanours then the algorithm was correct 61% of the time. More alarmingly, there is evidence that the algorithm is biased against racial minorities. Black and Latino defendants, both male and female, are labelled as high risk more often than white defendants. The algorithm overestimates the probability of reoffending by black defendants and underestimates the probability of reoffending by white defendants. Defending its algorithm, Northpointe claims that the scores are reliable when evaluated individually (Corbett-Davies et al. 2016). For example, 60% of white defendants who received a risk score of 7 out of 10 reoffended, and 61% of black defendants who received the same score went on to reoffend. Statistically, higher risk ratings do appear to correlate strongly with reoffending – those assigned a higher risk rate were four times more likely to reoffend than those who were assigned a lower risk rating.

Consider the following questions from the COMPAS questionnaire;[6] “How many of your friends/acquaintances have ever been arrested?”, “How often have you moved in the last twelve months?”, and “In your neighbourhood, have some of your friends or family been crime victims?”. The response options to these questions are simple approximations such as “never”, “some”, “once”, or “often”, which do not provide context or further explanation. However, these questions function as proxies for protected attributes such as race. For example, as of 2016, African American adults are 5.9 times more likely to be incarcerated than white Americans, and Hispanic Americans are 3.1 times as likely (The Sentencing Project 2018, p. 1). Where the COMPAS questionnaire asks about friends or acquaintances who have previously been arrested, it is statistically far more likely that a

[5] Notably, the questionnaires are different for male and female defendants, and the answers are compared only to the relevant gender in the database.

[6] As of late 2020, a copy of a completed COMPAS questionnaire is available at: https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html

defendant will answer yes if they have friends from black or Hispanic communities than if they have friends from white communities. Of course, while having a large number of your friends being arrested may indeed be a sign of gang affiliation, it may also simply be a sign that you are a member of a group who are over-policed and arrested more frequently than other groups.

The difficulty with these risk assessments is that they are often unverifiable. Should a defendant receive a higher sentence or have bail denied, then there is no way of knowing whether it is counterfactually true that the defendant would have reoffended during that time. For example, Paul Zilly was convicted in early 2013 of stealing a lawnmower and some tools. COMPAS assigned him a high risk score for future violent crime based on a history of methamphetamine usage (Angwin et al. 2016). The prosecution had offered a plea deal of one year in prison, and the defence had accepted the deal, but Judge James Babler overturned the plea deal based in part on the risk score and sentenced him to two years in prison. At an appeal hearing in late 2013, Judge Babler reduced the sentence to 18 months, stating that he would have initially given 18 months had he not seen the risk score at the sentencing hearing. We do not yet know whether Zilly's risk score was accurate but based on Judge Babler's own comments it played a significant role in extending the length of the sentence handed down. If it turns out that score was inaccurate, Zilly could have served an unwarranted 6-12 months in prison because of an erroneous prediction made by the COMPAS algorithm.

Power in Criminal Risk Assessment

The goal of power here is, to put it simply, the reduction of crime. For those risk assessment tools that are used during bail hearings, the aim is to reduce crime by denying bail to those who may commit crime while awaiting trial. With respect to those tools used for advising on sentencing, the aim is to reduce crime by keeping those likely to reoffend in custody. The agent of power here is the judge, as they are the primary decision maker within this context, though there are other, possibly competing, agents such as lawyers. The decisions that can be made by agents within the court room, including both judges and lawyers, will be constrained by laws, principles, and procedural rules, but they are still the agents of power in this context as they are the ones making decisions and exercising power over others. The individual who is standing trial is the subject of the exercise of this mode of power. While the goal of power here is to reduce crime across a larger population, each exercise of this power has as its subject the individual defendant on trial.

One of the primary means of this mode of power is the threat of sanctions, including both imprisonment and fines, differentiated according to the relative risk different individuals pose to the wider community. Those who are determined to be more likely to commit further crimes are subject to harsher penalties than those determined to be less likely to commit further crimes. A second mechanism for this mode of power is the interpretation and application of a rules-based system. The threat of sanction is not arbitrary, as judges are not free to impose any sanctions that they see fit. Instead, they must work within the legal system that sets out the punishments that may be meted out as well as the way those punishments can be determined. Instead, they must abide by sentencing guidelines. Related to this is a third mechanism which is that judges as agents of power here must have a knowledge of the rules of the system and be able to work with and around them in order to exercise power on the subject.

In this context, we can see the conceptual features of Weber’s account of power. As outlined earlier, three of the main features of Weberian power are first, that power requires a base of legitimacy such as legal authority or a legitimising bureaucratic structure, second, to exercise power within a system an agent needs both technical knowledge and a knowledge of the rules and procedures of the system they are working in, and third, that power can only be exercised on subjects who have a common membership to the system. In this context the court system is the bureaucracy, a system of hierarchies and legitimised rules that gives weight to exercises of power within the bounds of that system and authority to those in the higher ranks of the hierarchy, such as judges. To then exercise power, judges and other agents within the court room must have a command of technical knowledge of both the facts of a case and general legal principles, and a knowledge of the procedural rules of the court room through which they can exercise power. Using these knowledges, a judge can then as an agent of power issue a command with specific content, such as a sentence, and have it followed despite resistance. Finally, it is essential that both agent and subject be members of the system, which in court systems is usually a matter of jurisdiction. Where a court has jurisdiction to hear a case, it effectively takes the subject of an exercise of power to be a member of that bureaucratic system.

However, it is not just the conceptual features of Weber’s understanding of power we can see here. A pluralistic attitude towards power also allows us to appreciate the presence, and importance, of a key feature of Foucault’s account of power, namely dividing practices. The key dividing practice for Foucault was between normal and abnormal (Schirato et al. 2012, p. 59). In this context that division is between those who are normal, or not likely to commit further criminal activity, and those who are classified as “delinquents”, or likely to commit further criminal activity. As part of the operation of power, people are categorised as normal and abnormal, and those who are deemed abnormal are subject to legal processes designed to deal with that abnormality.

Just as with the examples considered earlier in Chapter 4, the use of big data in this context (and in the contexts considered below) has not generated a new form of power here and there are some clear historical continuities. There is a history of risk assessments being used in criminal trials in the US at least as far back as the 1920s. In fact, courts in every jurisdiction have a far longer history of attempting to assess the risk of an individual committing further crimes. Since at least the early 20th century, judges have exercised this kind of power, namely a kind of Weberian power with an element of Foucauldian power also present, in sentencing and bail decisions. The functions of a judge can only be exercised highly bureaucratised legal procedures, in combination with an in-depth knowledge of legal principles and material facts. In this sense, big data-based risk assessment tools can be seen as the application of current technology to longstanding juridical practices.

Where judges use big data as part of the exercise of power, some of the impacts discussed earlier are observed, such as an increase in the efficiency and effectiveness of exercises of power. The exercise of power is made more efficient, as decision-making processes are automated. In handing down a sentence or pre-trial conditions, a judge will often have regard to the kinds of considerations used in the algorithmic risk assessment tools. Algorithmic tools, such as COMPAS, can automate those evaluations by presenting the judge with a pre-calculated risk score. In this context, the risk assessment tools are providing agents of power with additional technical knowledge in the form of quantified predictions. The representation of these predictions as scientifically valid inferences can make the exercise of power more effective, by providing the appearance of objective evidential support for decisions that are made, which makes the exercise of power harder to resist or appeal.

There are also impacts on the operation of power as a result of the shift to the data double. As data doubles become more centrally important for identifying subjects for the exercise of power, the dividing practices here likewise become more important and are altered. The dividing practices that Foucault discusses are focused on individuals; on dividing normal from abnormal people. With the use of big data, the dividing practices are now operating on and through data doubles, creating data doubles to be evaluated as normal or abnormal, and then working to divide those individuals the doubles refer to. This Foucauldian feature of power becomes more important in this context, as it is now central to the operation of power.

The use of big data in this context also shifts the operation of power through the creation of a kind of "secondary" bureaucracy that works alongside the "primary" bureaucratic structure. This secondary system constrains the actions of agents, like judges, who exist within the "primary" bureaucracy. As part of a judge's decision-making process, they decide not just the length and nature of any custodial intervention, but also which defendants are eligible subjects for such an intervention. In order to assess the appropriateness of the subject and then exercise power on them, the judge needs both of the requisite knowledges of Weberian power, that is, a knowledge of the rules and procedures of the system, and technical knowledge, here of both legal principles and of the circumstances and details of the defendant and the case itself.

However, the use of algorithmic risk assessment tools disrupts the importance of knowledge to Weberian power by creating a kind of automated secondary bureaucracy, alongside the main bureaucracy of the court system, placing additional constraints on the decisions that judges can make.[7] The algorithmic risk assessment is automating one of the main types of judicial decisions, namely identifying who is an appropriate subject for custodial intervention. It also provides strong guidance on another type of judicial decision, namely the length and nature of the sentence. Traditionally, the judge will use both forms of knowledge in making these decisions, but the use of algorithms is automating aspects of this process. Additionally, the process by which algorithms generate a risk score may be opaque to the judge, who cannot see the process by which the score is generated. Consequently, although the judge is still the agent of power, they are now exercising power without full technical knowledge of how the determinant criteria of sentencing are produced. The use of data doubles here to identify subjects of power is locating aspects of procedure inside the black box of proprietary algorithms.

This shift to the data double makes it difficult maintain accountability over the exercise of

[7] Of course, at this point there is no evidence that any judge has made a decision based *solely* on an algorithmically generated risk score. But there is evidence that some judges are relying on them as part of their decision-making processes, and as they spread, they may become even more influential.

power in this context. Historically, accountability of these kinds of Weberian power depend on knowledge of the rules of the system. An exercise of power can be questioned or challenged when it does not follow institutional rules and processes. However, as decision-making processes become black-boxed through the use of algorithmic risk assessment tools, it becomes harder to keep power accountable. It is difficult check the validity of decision-making processes where those processes are not transparent, and where claims about the unbiased objectivity of algorithmic risk assessments are unverifiable.

A high risk score is effectively a prediction that a person is likely to engage in criminal activity in the future, but this prediction is inherently unfalsifiable. If that score is produced as part of pretrial hearings, and the defendant is held in police custody, then the prediction is never tested. If it leads to a harsher sentence, then the prediction increases the likelihood of its own accuracy. For example, placing an individual in prison for longer may make their economic position more precarious which may in turn precipitate further criminal activity in the future.

The algorithmic process gives the prediction of future criminal activity the appearance of being "scientifically" determined. The supposed objectivity of algorithmic risk assessment has been sold as a way to address the legitimacy crisis in criminal justice, but as Ben Green (2020, p. 595) argues, this is a false promise, as '… the objectivity promised by risk assessments is a chimera: rather than removing discretion to create neutral and objective decisions, risk assessments shift discretion toward other people and decision points.' Purely objective reasoning, as Green notes, is impossible, as there are sites of hidden discretion in the operation of algorithmic criminal risk assessments (Green 2020, p. 596). These sites of discretion are the defining of risk, the generating of input data, setting thresholds, and then responding to predictions. In each of these sites, individuals exercise discretion in the generation of a risk assessment, and the use of an algorithmic process serves to hide these sites of discretion, giving the exercise of power an air of objectivity because it has been "scientifically" determined. This not only makes it difficult to ensure that power is exercised in accountable ways, but arguably makes structural bias even harder to address by embedding it in opaque algorithmic processes.

Predictive Policing

Since the first days of the modern police force in the early 19th century, one of the primary purposes of the police has been the reduction and prevention of crime (Williams 2003, p. 10). To achieve this, the first modern professional police force, the Metropolitan Police of London, deployed beat police, and other police forces across the world soon followed suit. A beat police officer would perform regular patrols in the areas around their precincts, both gathering information to report back to their superiors and exerting a deterrent effect on criminal activity through their obvious and consistent presence. Over time, as police forces grew, there has been increased focus on ways in which policing can be made more efficient and cost-effective. While regular police patrols have remained a standard practice for police departments worldwide, limited resources and time means that officers must be deployed strategically. This has in turn led law enforcement agencies to try to predict the likelihood of criminal activity in particular areas in order to allocate limited resources as efficiently as possible.

To this end, police forces across the world, but particularly in the US, have embraced the use of big data to help predict criminal activity through various processes that can be grouped together under the term "predictive policing". Predictive policing refers to the use of analytical techniques to generate and act on crime probabilities (Degeling & Berendt 2018, p. 347), and can be used to solve past crimes as well as to identify targets for police intervention to prevent future crimes (Griffard 2019, p. 46). There are four methods of predictive policing:

1. Methods for predicting places and times of crimes.
2. Methods for predicting offenders and identifying individuals likely to commit crimes.
3. Methods for predicting perpetrators' identities.
4. Methods for predicting victims of crimes. (Degeling & Berendt 2018, p. 347)

There are many different tools currently used by police departments, but we will briefly look at three major examples.

The first example is that of Patternizr, which was developed for the New York Police Department (NYPD), and has been in use since 2016, though the existence of the program was only made public in 2019 (Griffard 2019, p. 44). Patternizr is an example of a big data-based tool that is used to predict which specific individuals may be responsible for unsolved crimes. The developers of Patternizr isolated 39 attributes or features that commonly appear in cases of robberies, burglaries, and grand larcenies. They then trained three models (one for each crime) on 10,000 patterns identified by NYPD analysts between 2006 and 2015, and the algorithm learned to weight different attributes to identify patterns between different crimes (Griffard 2019, p. 63). Practically, the software allows officers and police analysts to select a crime report from the NYPD to be "patternised" (Griffard 2019, p. 60). Key features of the crime report are identified by the algorithm, which then compares the report with other reports in the system. Patternizr produces a list of up to ten potentially related crimes that have each been scored between 0 and 1, based on the strength of the similarity. The analyst then decides whether to treat the group as a pattern, using information from one to assist in the investigation of others in the group, including predicting the identity of the perpetrator.

While Patternizr is designed to predict the identity of specific perpetrators, the Strategic Subject List (SSL) is designed to predict both the identities of those likely to commit crimes in the future and those who are likely to be the victims of violent crime. The SSL was initially developed by researchers at the Illinois Institute of Technology and was used in Chicago from 2012 until late 2019 (Charles 2020). The algorithms behind the SSL analysed data from the Chicago Police Department's arrest records, including the number of arrests and convictions, any gang affiliations, and status as the victim of a crime, as well as data about that individual's social network. The algorithm then weighted the data and produced a score between 1-500 indicating the likely risk that individual will be involved in violence as either a victim or an aggressor in the future (Asaro 2019, p. 46). The police have been very secretive as to how they used the list, only releasing information about the list itself in 2017 following a lengthy legal dispute with journalists (Kunichoff & Sier

2017). Initial implementation of the SSL contained data from over 398,000 individuals, including many who had never been arrested before but were included because they had family or friends who had been arrested (Asaro 2019, p. 46). Use of the SSL was also initially haphazard, with some officers making visits to those who were predicted as high risk to inform them that police were now closely watching them, while others used the system as a place to start investigations into criminal activity. The list faced vocal criticism before it was abandoned in 2019. Critics argued that using arrest information, rather than information from convictions, meant suspects were being identified based on crimes they may not have committed. Critics also pointed out that over 56% of black men aged 20-29, in comparison to 6% of white men of the same age, in Chicago have been arrested, largely as a result of historic police biases (Kunichoff & Sier 2017). When the SSL was decommissioned, the office of Chicago's Inspector General released a statement setting out the general concerns that lead to the shutting down of the program, including

> *…the unreliability of risk scores and tiers; improperly trained sworn personnel; a lack of controls for internal and external access; interventions influenced by PTV risk models which may have attached negative consequences to arrests that did not result in convictions…* (Charles 2020)

In effect, the Inspector General was largely accepting the critiques that were being directed at the program, admitting that the program produced possibly unreliable risk scores that potentially led to unnecessary and otherwise unwarranted arrests.

A third example here is PredPol, a predictive policing tool that is designed to predict the likelihood of criminal activity within a geographical area. PredPol is a predictive algorithm designed by researchers at the University of California Los Angeles (Degeling & Berendt 2018, p. 349). It functions on a theory of crime patterns called "near repeat theory", which holds that after the first occurrence of an event (such as a crime) the probability of a similar or identical repeat event increases. Research suggests that at least for some crimes such as burglaries this effect does occur (Degeling & Berendt 2018, p. 349). The PredPol algorithm examines historical crime data for an area and generates a prediction of how likely it is that a similar crime will be committed in that area, as well as a likely time frame in which that crime will occur. This allows police officers to be despatched pre-emptively to either prevent the crime or catch the offender in the act. As of 2017, the company behind PredPol claims that their system has effectively reduced crime rates in jurisdictions utilising their predictive software, including a 32% drop in burglaries and a 20% drop in vehicle theft in Alhambra, California since 2013, a 20% drop in predicted crimes in the Foothill division of Los Angeles, and a 15-30% drop in burglaries in just the first four months of use in Norcross, California (Kirkpatrick 2017, p. 22). While these statistics may seem impressive, it is difficult to assess whether these numbers are accurate. In part, this is because the algorithms that make up PredPol are proprietary, and are thus protected trade secrets, but also because it is difficult to establish the cause of any change in crime rates (Hvistendahl 2016). While some comparisons can be made with historic crime rates, the best way to assess the effectiveness of a program like PredPol is to compare outcomes where it is used to demographically similar areas where it is not used. This is a research tactic that law enforcement agencies are reluctant to use, as it would require them to effectively treat a section of a city as an experimental control, in which they would deliberately not use all the tools at their disposal to prevent crime. Without such a study, claims about the effectiveness of PredPol cannot be validated.

Power in Predictive Policing

Across all forms of predictive policing, the general goal of power is to reduce crime and promote order. For those tools aimed at predicting the identities of perpetrators like Patternizr, that goal is practically pursued by aiming to apprehend those who have committed a crime before they can commit another. For those tools aimed at predicting future criminal activity by an individual or within an area, like the SSL or PredPol, the practical aim is to exert a deterrent effect on specific individuals or more generally in designated areas. Regardless of the practical aims of each tool, the general goal is to reduce or prevent crime, and promote order. The agent of power is largely the police force utilising the predictive tools. However, in some cases such as PredPol where the predictive software is provided by an external group or company, that external group or company will also act as agents of power through their control of the software. The subjects of power here will differ based on whether the predictive tool is focused on an individual or on a geographic area. For those tools that make predictions about specific individuals, the subjects of power are those individuals with predictions made about them. For those tools that make predictions about crimes within geographic areas, the subjects of power are those individuals who live within or visit those areas.

For the means, the primary mechanism of power in this context is police intervention. How the police will intervene will change from case to case, and police interventions can take many different forms. They may range from increased remote surveillance, to increased physical presence and patrols, to direct engagement with individuals identified by predictive algorithms. Alongside these police interventions, a second crucial mechanism of power here is "targeted mass surveillance". For the operation of power in this context, it is necessary to collect large quantities of data about specific individuals and geographic areas. "Targeted" here refers to the use of surveillance on specific individuals or areas, and "mass" means the collection of as much data as possible about these targeted individuals or areas.

Alongside the primary mechanism of police intervention, a second important mechanism for the exercise of power here is the presence of a social relationship. The police force, and those officers carrying out the operation of power on a practical level, are in a specific kind of social relationship with civilians in their jurisdiction. The authority of police officers depends, in practice, on public acceptance of that authority. This social relationship is crucial for the operation of power, as that relationship both defines how the police can exercise power and how the public should respond to the exercise of power by police. A further important mechanism in those cases where predictions are made about future crime within a geographic area, which is a generalised threat of police force. The visible presence of police officers in an area has a deterrent effect.

The police force is a complex institution and there are many distinct dimensions to police power. For the purpose of this discussion I want to focus on Dahl's analysis of the nature of police power and the way this is being affected by predictive policing. The essential features of Dahlian power are the presence of a social relationship, conflict between two parties whereby the will of one will prevail over the other, as well as a definable base, means, scope and amount of power. All of these elements are present in this context. Police forces and civilian populations are part of a complex social relationship, in which there are often conflicting desires and interests between police and civilians. As the police act, their actions induce the performance of or avoidance of behaviour by those being targeted by power. There is also a direct way in which this power can be measured: as the police begin surveillance of an individual, communicate with them directly, or undertake some other intervention, their actions can be assessed with counterfactual reasoning as either effective or ineffective at preventing that individual from committing some future crime.

As discussed above, there is a history of police trying to predict criminal activity, so that limited police resources can be used effectively to prevent crime. From the early days of the modern police, officers on patrol would report back information about the areas they patrolled, which informed where future patrols would take place. By the mid-19th century, the London Metropolitan Police were compiling reports about the numbers of known thieves, prostitutes, suspected persons, vagrants and tramps, as well as houses of bad character observed within the areas they patrolled (Williams 2003, p. 29). These practices continued, and over time theories emerged as to how best to predict rates of criminal activity, such as the notorious "broken windows" theory of policing from the 1980s (Childress 2016). This theory held that high rates of petty crimes such as vandalism or loitering would lead over time to more serious and violent crimes. With the development of big data, however, these predictive efforts have been supercharged, and the operation of power has been transformed.

The use of big data to predict whether an individual has committed a crime or is likely to commit a crime shifts the operation of Dahlian power in two main ways. Firstly, data doubles become a central part of the base and means of power, as well as impact on the scope and amount of power, in Dahlian terms. They become the base of power, in that they become the justification for an exercise of power. The selection of an individual by a predictive algorithm becomes a reason for exercising power on that individual. Predictions also become a central part of the means of power. An individual may be threatened or arrested by the police, and as part of that threat or arrest the police may say that they have reason to believe that that individual poses a risk of criminal activity. For example, while the SSL was in use in Chicago, police officials would often cite the scores generated by the SSL to reporters when discussing high profile cases (Gorner & Sweeney 2020). The prediction is incorporated into police tactics for exercising power. The predictions of the data double also become important parts of how we determine the scope of power, that is, the responses available to the subject of power, and the amount of power being exercised, or the likely successfulness of power. If the prediction indicates a high risk of offending, or of a particularly violent crime, then an individual will have a more restricted scope of actions available to them, and the exercise of power will likely be more successful (e.g. a prediction of a higher risk may lead to an arrest, whereas a prediction of a lower risk may not, as a prediction of a higher risk of criminality will justify the use of more police force).

The use of the data double as an actuarial tool, to predict risk and identify individuals to be subjected to power, also fundamentally alters the nature of the social relationship at the heart of Dahlian power. Consider the first example that Dahl offers as an intuitively compelling instance of power, where a police officer is directing traffic (Dahl 1957, p. 202). The police officer can stand in the middle of the road, wave his or her arms, and command the traffic around them to move in certain ways, because of the social relationship between the public and the police. If I stand in the road and wave my arms, I will not achieve the same effect, as I am not a police officer and do not possess that form of social authority. But the use of data doubles alters this social relationship. Individuals are being identified for police attention in a new way, not strictly by police but by automated algorithmic analysis. Dahl's point is that the power exercised in legitimate policing depends on public acceptance of that power. As the relationship between the police and the policed becomes mediated by databases and algorithms, the social relationships that constitute a basis of police power will be transformed, with potentially damaging implications for the legitimacy of police power.

As an instructive example of how the social relationship between the police and the public is changed from the use of big data, consider the use of social media as a data source for predictive policing tools, especially with respect to prospective protests and riots. Following widespread protests and riots sparked by the shooting of an African American man by police officers in Ferguson, Missouri in 2014, a report by the US Department of Justice's Office of Community Oriented Policing Services determined that 'Social media was the key global driver of the Ferguson demonstrations.' (Binder 2016, p. 245). In response, many police departments across the US began to monitor social media more closely to identify and respond to calls for demonstrations or riots. As part of this surveillance, data-mining tools have been used to monitor and assess the sentiments of the public (both as a whole and by targeting certain demographic groups), to predict the likelihood that demonstrations or violent riots will break out (Binder 2016, p. 246).

The expression of political opinions on social media is not socially understood as raw data for predictive policing, but such data sources are of considerable value for predictive analysis. From otherwise lawful communications, protected in the US by rights to freedom of speech and rights of (peaceful) assembly, predictive policing tools are constructing data doubles that make individuals, groups, or locations into targets for pre-emptive policing. As these data sources are co-opted for predictive risk assessment, the operation of police power changes, and the concept of probable cause is radically eroded.

The exercise of police power, as part of the social relationship between the police and the public, depends on an acceptance by the public that police power is legitimate, that it is being exercised with the consent of the public and for the benefit of the public. To ensure this, there are several important limitations built into the kinds of power available to police forces, and in the US one of these limitations is the requirement of probable cause. Probable cause is a legal standard that must be met for a police officer to obtain an arrest or search warrant, and to act on these warrants. Probable cause requires more than mere suspicion of criminal activity; it is met if a reasonable person would believe that crime is being, has been, or will be committed.

Where big data is used to construct data doubles of individuals, be that from social media data when trying to predict violent demonstrations, identifying geographical areas in which criminal activity will occur, or identifying specific individuals as suspects in criminal investigations, the use of the data double as part of the exercise of power changes the nature of probable cause. An arrest or other police intervention may not be based on the belief of a "reasonable person", but on an algorithmically generated risk score. Probable cause is a fundamental limit on the operation of police power and a key way in which police forces are held accountable, and it is being undermined as data doubles are used to identify subjects of police power. This in turn may erode public trust in the police, and radically change the social relationship between the police and the public.

This change in probable cause is even more concerning when considering the ways in which predictive policing tools can embed existing structural biases in ways that make them harder to identify and address, further undermining the legitimacy of police power. The databases that are used as part of predictive policing provide an 'incomplete and unrepresentative picture of all crimes' (Griffard 2019, p. 49), as police data is often informed by both the implicit and explicit biases (particularly racial biases) of police and community members, based on where police patrol and who they interact with, as well as which community members report criminal activity. At its worst, 'Offender-based predictions exacerbate racial biases in the criminal justice system and undermine the principle of presumed innocence. Equating locations with criminality amplifies problematic policing patterns.' (Shapiro 2017, p. 458).

Targeted Political Advertising

One of the most widely discussed applications of big data is its use in marketing for targeted advertising. Targeted advertising, or as it is sometimes called "online behavioural advertising", works by targeting advertisements at individuals based on data collected about that individual's preferences (Boerman et al. 2017). Most commonly this data is collected through browsing history and other online activities, but increasingly this data is obtained from offline activities such as participation in loyalty programs or mobile phone GPS location tracking. As a simple example of how a targeted advertisement might be served, someone might visit a website about cars, watch a YouTube video about car maintenance, and visit a car dealership in person carrying their mobile phone. As they complete those activities, they leave behind a trail of data, which is captured and used to create a profile about that individual. Based on that profile, they are then served advertisements for cars or car parts, as the system has categorised them as someone likely to purchase a car or car-related accessories. While there are legitimate concerns around the use of targeted advertising in commercial settings, this discussion is concerned with the use of targeted advertising in political settings, particularly during election campaigns.

Political advertising is not new; indeed, it has long been an essential part of running an election campaign. But in recent years, campaigners and political parties have turned to big data to increase the precision and cost effectiveness of their campaign advertisements. One company to provide such a service was Cambridge Analytica, a data analytics and advertising company, which came to public attention during the 2016 US presidential election. The Cambridge Analytica (CA) story begins in April 2010, when Facebook launched a new platform called Open Graph (Meredith 2018). Open Graph allowed third party developers to directly request the personal data of Facebook users, including their name, date of birth, location, all publicly listed information, and even their private messages, which developers could then use. The Open Graph platform prompted a proliferation of apps, including quizzes and games, giving users new experiences on the Facebook site, and initial resistance to Open Graph quickly faded. One such app was MyPersonality, developed by David Stillwell and later by Michal Kosinski, researchers from Cambridge University (Grassegger & Krogerus 2017). The MyPersonality app was developed as a research tool where users answered psychometric and psychological questionnaires. The answers to these questionnaires were compiled and compared to individuals "likes" on Facebook and formed the basis for research demonstrating that it is possible to predict basic demographic attributes and personality traits from an individual's likes on Facebook. For example, their model could distinguish between heterosexual and homosexual men with 88% accuracy, between African Americans and Caucasian Americans in 95% of cases, and between Democrats and Republicans in 85% of cases, and even approached the accuracy of standard personality tests to determine personality traits like "openness" (Kosinski et al. 2013). The model was also able to predict, with less certainty but still better than chance, whether an individual's parents were divorced, whether they use drugs, and even their intelligence.

In 2014, Kosinski was approached by an assistant professor of psychology at Cambridge, Aleksandr Kogan. Kogan had ties to a company called Strategic Communication Laboratories (SCL), who billed themselves as the 'premier election management agency' and provided political marketing based on psychological modelling (Grassegger & Krogerus 2017). SCL was interested in Kosinski's research and methods, and wanted to access the MyPersonality database, but Kogan could not tell Kosinski what they would use that database for. Kosinski ultimately declined to share the database with Kogan and SCL but inspired by Kosinski's methods Kogan developed his own Facebook app: "thisisyourdigitallife". Just like its inspiration, Mypersonality, users of thisisyourdigitallife answered personality tests and psychographical quizzes. While thisisyourdigitallife had roughly 270,000 users, it was developed at a time when the Open Graph platform allowed developers access to not just the data of users, but also the public data of any friends of the users of the app, including name, age, location, "likes", and more. As such, Kogan was able to develop a database with data points on some 50 million Facebook users, despite only 270,000 users directly consenting to sharing their data. At the time, this data collection was within the terms of use of the Open Graph platform, but any collected data was not to be shared with an external data broker or other advertising agency. Despite this, Kogan shared this database with the newly incorporated CA, a subsidiary of SCL, who immediately put that data to use in the run up to the 2016 US Presidential Elections.

In late 2015, Republican presidential candidate Ted Cruz had contracted CA to assist with his presidential primary campaign (Grassegger & Krogerus 2017). CA obtained personal data on voters from as many different sources as possible, including data from public sources like land and automotive registries and from private sources like grocery store loyalty card programs, magazine and email subscription services, and online apps and websites. Once that data was obtained, it was aggregated with lists of registered Republican voters, allowing for detailed personality profiles to be built based on the research they had performed with data obtained through thisisyourdigitallife. These profiles allowed Ted Cruz's primary campaign to target not just broad demographics e.g. women, African Americans, voters 65+ years old, but specific individuals based on precise psychometric profiles. While Cruz did not go on to win the Republican Primary, CA certainly played a role in boosting Cruz from relative anonymity to a competitive position in the primaries. At the start of the primary race, less than 40% of the general population had heard of him and he went on to win the Iowa primary, which is often considered the most important state to win (Grassegger & Krogerus 2017). Following Cruz's defeat, then-Republican nominee Donald Trump hired CA to work on his presidential campaign. Post-election analysis suggests that CA's work was influential in Trump's victory in the 2016 election, though it is difficult to say whether he would have won without them.

While we may never know for sure exactly how important CA was in Trump's election strategy, his opponent Hilary Clinton said after the election 'You can believe the hype on how great they were or the hype on how they weren't, but the fact is, they added something … They married content with delivery and data. And it was a potent combination.' (Wood 2017). CA allowed the Trump campaign to test up to 175,000 advertisement variations in a single day, releasing advertisements that differed in only tiny details ranging from the pictures and videos used to the exact wording of the heading, the colours used in the advertisement, and most importantly the individuals who got to see the advertisements. Just as with Cruz's advertisements, they were specifically geared towards individuals with specific messages that were calculated as the most likely to prompt them to vote, or more controversially scare them away from voting (Green & Issenberg 2016). This targeted advertising was not just delivered online, but also in person; CA's data empowered door-to-door canvassers with an app identifying the political views and personality types of the members of households they were visiting, allowing them to specifically target households with personalised messages for maximum impact. Importantly, CA's data did not significantly contribute to advertisements run by either Cruz or Trump in newspapers, magazines, radio, or television. What these mediums lack that enables this strategy online and in person is the ability to target the individual. In the traditional mass media formats, many people of different demographics will consume the same media content, making this kind of big data driven targeted advertising difficult at best and impossible at worst.

Power in Targeted Advertising

The goal of power here is to win an election. Largely this will be achieved by persuading undecided voters to vote for a particular person or party, but it may also involve dissuading people from voting. While any individual advertisement will be presented with the goal of changing the voting behaviour of a specific person, ultimately the end goal of this mode of power is to win an election by securing the majority of votes. The agent of this mode of power is the candidate or political party who is campaigning for election. Many, if not all, political actors who will be employing this mode of power will be relying on the technical expertise of a third party, just as with

Cruz and Trump employing CA to run their advertising campaigns. But even though it is often a third party who is running these advertisements, the agent of power here is the political campaign they are working for. The subjects here are the voters.

As to the means of this mode of power, one of the main techniques is the making of threats and promises to the subjects of power. As part of the election campaign, candidates will typically make indirect threats about what will happen if their opponent is successful, as well as make promises about what will happen if they are successful. These threats and promises are calculated to sway the subjects of power to vote or not vote in certain ways, in order to secure a win in the election. To make these threats and promises this mode of power relies on techniques of profiling and manipulation. In traditional electoral advertising, this profiling is performed through demographic analysis, looking at blocs of voters based on characteristics such as age, gender, race, registered voting preferences and employment. These groups are then used to guide the crafting of threats and promises that are being made. For example, to encourage suburban women to vote for a candidate they may make promises or threats calculated to appeal to suburban women voters. The psychographic characteristics of these voter blocs are used to facilitate a form of psychological manipulation, to motivate individuals to votes in a particular way.

In this context, we can see the conceptual features of Machiavelli's account of power. The key feature of Machiavellian power is that there is a competition between parties, which is at the heart of the operation of power in this context. The agents of power here are quite literally engaged in a contest over power from which one will emerge as the winner, and they must engage strategies and exercise other forms of power and manipulation to win that contest. From there, the making of threats and promises as well as psychological profiling and manipulation are hallmark techniques of a kind of Machiavellian power. Of course, Machiavelli does not explicitly anticipate the kind of political campaigning that exists today, and many of the strategies he discusses in *The Prince* are focused on autocratic governance, but the contextual features of the mode of power here directly indicate the presence of Machiavellian power. Finally, we see that power is comparative in nature, in that a person with more power has a greater scope for action in relation to others. This is true both in the sense that the eventual winner in the contest will have a greater scope of action, and in the sense that during the contest itself those parties with more power are those who have the greater scope of action against their opponents, whether that be a greater capacity to control the media, more funds to spend on advertisements, or more data collection and analysis to inform those advertisements.

Of course, political advertising did not start with the development of big data, and the idea of trying to win over a population to support a ruler is ancient. Modern elections have become highly dependent on marketing, where candidates are presented to the electorate as a kind of product to be "purchased" and this trend has accelerated since the development of mass media. Traditional (pre-big data) political advertising is aimed at relatively large blocs or demographic groups: rural voters, minority voters, women voters, LGBTQIA+ voters, etc. These traditional advertisements are still geared to changing human behaviour in terms of individual voting preferences, but they are built to target demographic groups. Largely this is because of practical constraints, as political advertisements conveyed by traditional mass media, such as newspapers, radios, and televisions, cannot be tailored to individual viewers, but must be broadcast to larger groups. But with the introduction of big data, the exercise of power here shifts away from demographics and towards psychographics; away from group psychology and towards individual psychology. In other words, a shift to data doubles. Targeted advertising works through constructing data doubles in the form of psychometric profiles. These doubles take fragments of demographic data about a person and combine them with psychographic data, such as opinions, preferences, likes and dislikes, etc. From this data, inferences are made about aspects of the individual the double represents, as well as predictions about what messages will induce them to vote a certain way or not vote at all. The effectiveness of targeted advertising has been greatly enhanced by social media platforms which, unlike traditional media, enable messages to be directed to be directed to highly specific audiences based on these psychometric profiles.

As an example of the difference between traditional and targeted political advertising, consider advertisements around gun rights. Traditional advertisements about gun rights would be aimed at broad demographic groups, such as Republicans, black voters, men, etc, and the messages of these advertisements would be constructed to appeal to as much of the demographic as possible. But the use of data doubles allows for tailored advertisements calculated to sway individual votes. Let us look at two advertisements that CA ran as part of Cruz's campaign (Grassegger & Krogerus 2017). Cruz had for many years been against the regulation of firearm ownership and had run advertisements to inform voters of these views. Individuals whose psychographic profiles indicate high levels of neuroticism or conscientiousness, or who are living in or near an area with a recent spike of violent crime, were shown advertisements on Facebook using threatening images of intruders alongside messages centred on the protection of family members, the home, or other private property. However, those whose profiles indicated a strong sense of tradition and family values, were shown advertisements featuring pictures of families hunting ducks together at sunset with messages focused on conservative values, small government, and hunting. These advertisements are highly effective manipulation tools (Wood 2017). They are uniquely personalised, targeted at characteristics of an individual that they may not even consciously realise about themselves, steering them towards a particular action.

Crucially, it is not the person who is being directly targeted. It is their data double that predicts their manipulability, which is targeted by the algorithm and thus the operation of power. While it is the individuals represented by those data doubles that see the advertisements, they are seeing specific advertisements based on a prediction of what will best manipulate them into performing a certain action like voting. These political advertisements are minutely targeted – a campaign manager can select all doubles that predict high levels of neuroticism, conscientiousness, or recent experience of violent crime. Or they can select all doubles that predict conservative and traditional values around family structure. They are not selecting the individuals directly, rather they are selecting and working on predictive data doubles.

On a surface level, this increases the efficiency and effectiveness of power, as power is now operating based on predictions that are more accurate and tailored than ever before. Traditional political advertising was still based in part on predictive analysis, namely attempting to predict how different messages will be received by different demographic groups, but the collection of data to support that analysis was slow and costly. With big data however, the collection of data is in near real time, specific down to the individual, and if not free then at vastly reduced costs. The predictions generated with big data are arguably far more accurate and precise than those achieved with traditional analysis techniques, further increasing the efficiency and the effectiveness of exercising power in this context. The use of big data also changes the range of power, allowing for power to be exercised through threats and promises targeted to individuals rather than to broader demographic groups.

However, there is a more fundamental shift in the operation of Machiavellian power in this context. Machiavellian power traditionally takes a hold of its subjects by threatening violence on or promising something to the subject of power. The violence threatened or reward promised may not necessarily be directed at the subject, for example a Machiavellian strategy may threaten violence on or promise a reward to a subject's family member, or even on some unrelated person or group. But the threat or promise is made to the subject, so that their actions are constrained by that threat or promise. But where Machiavellian power operates in the context of targeted political advertisements, the threat or promise is made based on the data double, rather than a human subject. As the data double is treated as real by the algorithm, the threats and promises that are made, such as those in the advertisements used by the Cruz campaign discussed above, are made based on the data double. They are crafted specifically to trigger a change in behaviour in that data double based on the predicted triggers of that data double for a change in behaviour. The threat or promise made based on the data double becomes the foundation of the choice architecture that is built around the individual. The individual is nudged based on what is determined as likely affect the data double in the desired way, and the success of the nudge is measured by observing a change in the data.

This shift poses significant problems for accountability in the context of targeted advertising. With respect to Machiavellian power, it may sometimes be more difficult to ensure accountability in the exercising of power in comparison to other kinds of power, largely because of the nature of power as a kind of contest over increased scope of action. However, where the exercise of Machiavellian power takes place within a recognised space of contest, such as in an election, there are ways in which we can ensure that power is exercised with accountability. To do so, we may use regulations around how power can be exercised with attached sanctions for violations, e.g. with political advertisements many jurisdictions have laws requiring disclosure of who authorised that advertisement and how it was funded, or prohibiting the use of certain tactics like outright slander. In doing so, we are imposing ways in which we can ensure that power is monitored and can be justified, and sanctions for the abuse of power can be enforced. But our ability to ensure accountability in this context is undermined by this revolutionary shift in the operation of power.

Targeting data doubles as the direct subject of power makes it very difficult to monitor power. As data doubles are targeted with tailored advertisements, it becomes difficult for individuals to see what advertisements are being shown to others. In traditional mass media, where one message is broadcast, members of different demographic groups are likely to see messages intended for groups that they are not a member of. This then allows them to assess and monitor the strategies being used by candidates within the election. But as advertisements are targeted to data doubles, and the individuals those doubles represent see tailored advertisements, it becomes harder to assess and monitor the strategies of candidates, as the messages being sent out are ideally only seen by those they are perfectly tailored for. This makes it very difficult to monitor exercises of power in this context as agents work to manipulate the behaviour of voters.

The shift also makes it harder to challenge the exercise of power in this context, as a sense of objectivity hides the competitive nature of power as Machiavelli sees it. The essential nature of Machiavellian power is that it is competitive, it is exercised as part of a contest between agents looking to secure a greater scope of action. But where decisions are made based on the kinds of predictions that big data allows, those decisions are given a veneer of objectivity which hides part of or all the competitive nature of those decisions. They no longer look like strategies employed to win a contest, but objective responses to the facts of the world. This makes it hard to challenge or enforce sanctions against any exercise of power here.

The shift to the data double also largely removes the need for agents of power to justify their exercises of power. As power is targeted at the data double as the subject, while a human will still see the political advertising it is harder for that human to notice the operation of power. For example, a data double may predict high levels of neuroticism which an individual may not have recognised within themselves, and when served an advertisement that targets these high levels of neuroticism, they may not be able to recognise that they have been nudged by the operation of power. The choice architecture around them may be such that it is entirely invisible. In situations such as these, no justification is necessary because none will be demanded. However, there is the chance that the predictions will be wrong, and an advertisement will be shown to a person based on a predicted attribute they do not in reality have. In this or similar situations, they may notice the attempt to build a choice architecture around them and may demand a justification for the exercise of power. But in these cases, the agent of power (or their representatives) may be unable to give that justification, because of the black box character of algorithmic analysis. Targeting data doubles as the subject of power makes power largely invisible to people who are successfully impacted by it, but for those who notice and demand an explanation, that same shift to the data double makes power opaque to the agent who cannot then access the reasons as to why that person was impacted by the operation of power. The predictions, the analysis, is performed within the confines of the algorithm, and are largely inaccessible to even the agent of power. In this way, the ability to justify exercises of power is undermined in this context.

Smart Cities

Urban landscapes have long been mediated by technology, but the phrase "smart city" only emerged in 2008 (Willis & Aurigi 2018, p. 8). In the years since, the idea of the smart city has grown immensely popular, however, despite its popularity a single definition has yet to emerge. Some definitions focus on networking; on linking together infrastructures like transport, energy, lighting, and a wide range of public and private services (Willis & Aurigi 2018, p. 9), while others focus on the use of sensors and digital surveillance built into the urban environment (Kitchin 2014b, p. 2). Other definitions look to avoid focusing too narrowly on the technology that makes up the smart city, and instead emphasise the ideal of the smart city as a city that uses digital technologies to optimise its functions and the quality of life of its inhabitants (Picon 2015, p. 29) or position the smart city as one that is forward-looking, using information technologies to drive sustainable growth and enhance quality of life (Gascó-Hernandez 2018, p. 52). Across these definitions, we can see the smart city as a kind of digitalised urban landscape, where interconnected infrastructures and sensors are used by both the city and its residents to promote economic growth and greater quality of life.

We can also distinguish between different models of construction (Pillania 2018; Wood & Mackinnon 2019, p. 177). Firstly, there are smart cities that have been built ex novo, like Songdo, South Korea, and Masbar, Dubai. These new smart cities are a contemporary version of mid-20th century projects like Chandigarh, India, and Canberra, Australia. The second model of construction of a smart city is the retrofitting of existing cities. Cities like Rio de Janero, Brazil, and Chicago, US are examples of retrofitted cities, where sensors and networks are attached to existing infrastructure to "make them smart". We can also see hybrid cities, such as the city-state of Singapore, which has been rebuilding the city to integrate digital technologies. Finally, we also see cities that create new smart districts or precincts within an existing city. This model is typically funded by private companies or interests, such as the Toronto Quayside precinct in Toronto, Canada, which has been developed in partnership with Google's Sidewalk Labs. The smart city, according to some writers, is also an idealised neoliberal project (Kitchin 2014b, p. 2; Wood & Mackinnon 2019, p. 177), whereby technological and market-led solutions to problems of governance are prioritised.

While some writers are cautious to avoid narrowly defining the smart city in terms of the technologies they use, it is still essential to examine some of the technologies used by smart cities and how they interact with and operate on the residents of the smart city. The most common technologies in smart cities are the millions of sensors used to both provide information to and gather information from residents. For example, Barcelona, Spain, utilises a host of these sensors to track the watering of plants in city parks to save maintenance costs and conserve water, to track buses on roads to provide for real time information on timing at bus stops, and sensors on street lights to allow for lights to activate automatically when detecting a passer-by and to allow for authorities to remotely attract or deter people from areas or events (Tieman 2017). Songdo International Business District in South Korea, a smart city built from scratch on 600 hectares of reclaimed land, features buildings with low U value windows, LED lights, water-cooled air-conditioning systems, solar energy panels, and connected television conferencing capabilities that can all be controlled remotely, and of course provide data back to the city and owner (Moser 2013, p. 24). Songdo also features a smart garbage collection system, where buildings are connected through a series of pneumatic tubes. Residents sort their waste into special bags, insert them into the tubes in their buildings where sensors either accept or reject the waste, before sending them through a network of pneumatic tubes to incineration or recycling plants (Neidhart 2018).

Several smart cities across the world feature technology from Playable Cities, who first started in Bristol, England. Playable Cities reimagines facets of urban infrastructure as opportunities for play using sensors, projections, lighting, and sound. The games include Shadowing, where street lights remember and play back shadows they cast, Urbanimals, where projections of wild animals appear across the city and invite passers-by to play with them, and Stop, Smile, Stroll, where facial recognition cameras at pedestrian crossings invite pedestrians to smile while waiting to cross the street (Watershed 2019). Berlin, Germany has also begun experimenting with tracking cars not just for traffic updates but also for weather updates. The team behind the navigation app HERE WeGo is working with the city by using sensors to detect when cars turn on their windscreen wipers or fog lights to provide the city and residents with live weather data across the city (Wright 2018). Across all these technologies, and the other technologies that go into the smart city, there is a focus on "datafying" the city, on making that data accessible to all stakeholders including citizens, governments, businesses, and academia, and on increasing participation and efficiency in the city.

The data gathered from these myriad sensors are then used not only to model the city and its residents, but also to guide or control the operation of the city and its residents. In Barcelona, motion sensors were attached to streetlights, originally with the aim of saving money by turning lights off when no one was walking along the street. However, city authorities began to use these sensors to attract people to certain areas during events, guiding the movement of pedestrians around the city (Tieman 2017). The Intelligent Traffic Signal System has been implemented in several American cities, including Arizona, California, and New York City. The system collects data from cars in real time to manage traffic and optimise traffic light cycles by detecting where there are high concentrations of cars as well as the directions and speeds they are travelling (Chen & Mao 2018). As well as simply collecting this data, the system can then be used to control and direct traffic around the city, prompting drivers to take alternative routes by controlling the speed of traffic lights to influence the flow of traffic.

Many of these technologies also create a kind of social pressure to remain connected. As pedestrians are guided by remote controlled streetlights in Barcelona, they are pressured to participate socially, and remain out where data on their movements can be collected. The games of Playable Cities are direct invitations to participate and play with others, especially those games that involve the faces of participants such as Stop, Smile, Stroll. They also create a sense of dependence, usually by offering convenience to the residents of the smart city. In Songdo, the automated recycling processes eliminate the need for garbage trucks, new buildings are constructed with climate control systems that can be operated at a distance by a mobile phone, and as many systems are connected and automated as possible. The combination of these technologies means that many aspects of private and public life are made highly convenient and efficient for residents, rewarding them for participating in the smart city. As individuals use the infrastructure of smart cities, they become reliant on these processes and incorporate them into their daily activities.

Power in the Smart City

In the context of the smart city, the goal of power is to optimise and streamline the operations of city. This optimisation can be the result of architectures or technologies that simply increase the efficiency of existing processes, such as improved road layouts or sensors for watering plants in Barcelona, but in many cases the pursuit of this goal will take the form of attempts to alter the behaviour of the residents of the city. Using lights to attract people to certain areas, hostile architecture in the form of benches with extra armrests or decorative lumps/spikes on window ledges, and using data to control the flow of traffic are some examples of the ways in which the goal of power here involves controlling and altering the behaviour of individual residents. The agent(s) of power in this context are those responsible for setting out or designing the city, whether that be city governments, urban planners, or other corporations who offer tools and expert advice. The subjects are the residents, visitors, and other inhabitants of the city itself.

Regarding the means of power here, the most important technique of power in this context is the use of architecture. Building and arranging the city in a certain way is the best way to ensure changes in the behaviour of the city's residents. Setting out roads in a certain layout will encourage people to move around the city in certain ways, metal bumps on stair rails will make it difficult for people to grind skateboards down them, additional arm rests in chairs will stop people from sleeping on park benches, and so on. The use of surveillance is another crucial technique of power in this context. This is true of the smart city, as it teems with sensors and data collectors, but also for city design pre-big data. To assess the success of the design of the city it is necessary to observe how residents are moving, by conducting surveys, polls, or just by watching the residents themselves. This surveillance both assesses the existing city design and informs future changes to the city, which are both crucial to exercising power in this context.

By analysing the mode of power in this context, we find a complicated overlapping of key conceptual features of several theoretical accounts of power. Firstly, we see some of the key features of Foucault's account of power, primarily that power operates as a productive force, that it is diffuse in nature, and it relies on constant and sometimes overt surveillance. The residents of the smart city are being shaped by the operation of power over time to be more ideal residents of the city and more normalised and productive than they were before. Power is also diffuse in the context of the smart city, particularly as it is the architecture and interconnected infrastructure of the city that manipulates and nudges individual behaviour. While it is best to identify the agent of power as the city leaders or those behind the design of the city, it is the architecture of the city that residents interact with and that serves as an interface in the exercise of power, and as such it is better to say that power operates diffusely through the design of the smart city itself. For power to function in this context then, there is a constant web of surveillant techniques across the city, some covert but many overt, making the residents aware they are being watched along the way.

Apart from the features of Foucault's account of power, we can also see key elements of Hobbes' and Lukes' accounts of power here, overlapping and intertwining with the kind of Foucauldian power being exercised here. From Hobbes' account of power, we can see the key feature of power operating in a way that is self-reinforcing. Those who get to decide on how the city is laid out and how data is collected and used will find themselves exercising power which is self-reinforcing, as they will be in a better position to control and organise the city the more they control and organise the city. We also see key elements of Lukes' account, in particular the third-dimension of power, as power works to reinforce the status quo and the exercise of power is accepted by the residents of the city as natural and normal. Beyond looking to train individuals, the exercise of power to increase the productivity of the city acts to maintain the status quo and prevent disruptions to the system. In doing so, it looks to operate in such a way that the exercise of power seems natural and normal, as if the city is just arranged that way and there is no power being exercised in the first place. These features of Lukes overlap with the Foucauldian elements here in an interesting way. Normally, an exercise of a kind of Foucauldian power relies on constant and overt surveillance, but as power here works to preserve the status quo and seem as normal as possible, the overt nature of surveillance is no longer necessary, and constant but covert surveillance can be utilised instead.

This mode of power has been in operation as long as cities have existed, but really began to grow in importance at the turn of the 19th century as London became the first city with over one million residents. As cities around the world continued to grow, there was a growing need to focus on managing the mass movement of people and other flows (e.g. energy, food, waste) across these urban landscapes. To avoid a large city becoming frozen by the number of people living within the urban space, the city itself must become as efficient as possible in moving those people and the things they need. As such, power is exercised to alter the behaviour of individuals within the city, often by using the architecture of the city to encourage individuals to act in certain ways. The development of big data has unlocked new ways for city planners and leaders to influence and modify the behaviour of the city's residents, which in turn leads to a shift in the operation of power in this context.

Big data allows for the real time micro-management of the city, both in terms of constant real time data collection and the manipulation of the infrastructure of the city. The constant stream of data in combination with the connected nature of the infrastructure of the smart city means that the designers and leaders of the city can actively control and adjust the influences that are being exercised on resident's behaviour, rather than trying to design elements of the city in advance to do the same thing over time. This leads to exercises of power being far more efficient and effective. While there are initial costs associated with the transformation of a city into a smart city in the form of the costs of installing sensors or rebuilding infrastructure to enable the smart city, the ability to then monitor and manipulate the city in real time makes the exercise of power much more cost effective. It also makes the exercise of power stronger, as changes in the environment can be made with near immediate effect.

There is also a more fundamental shift in the operation of power here as the result of this micro-managing being performed on data doubles, not on human individuals. As individuals move around the city or otherwise interact with the infrastructure of the city, data doubles are constructed about them, which in turn are used to make predictions about their future behaviours. They are used to see which individuals may be drawing close to an area of the city that is not optimal for them to approach, and then street lights may be activated strategically to nudge pedestrians away from certain areas and towards others while traffic lights may be slowed down or sped up to direct vehicle traffic away from certain areas and towards others. Exercises of power in this context are being targeted at data doubles, at the predicted actions and behaviours of the data double. The city residents are then nudged to conform to these predictions. If the city predicts that a critical mass of data doubles will drive in a certain direction, then traffic lights can be altered to stop that prediction from coming true. This exercise of power is targeted at those data doubles, it acts on the predicted doubles moving around the city, but it is the individuals those doubles represent who find themselves nudged to conform.

Foucauldian power, in many ways, already functions through nudging. The paradigmatic example of Foucauldian discipline, the panopticon, is essentially a choice architecture. The setup of the physical and non-physical aspects of the panopticon nudge the inmates over time to self-regulate and train themselves as subjects of power. However, Foucauldian power and the nudges that make it up operate on the body. The surveillance in the panopticon is of the body, the operation of power in the factory is in positioning the body in time and space, the observation of the body in the clinic. By surveilling and tracking the body, Foucauldian power over time nudges the individual to train themselves as subjects of power. But in the context of the smart city, the operation of Foucauldian power is disconnected from the body, and instead it surveils, and targets, data doubles. The body is not positioned in space or time, or directly controlled in the same way as traditional forms of Foucauldian power would position or control it. Data doubles of the residents are monitored and manipulated, which in turn nudges those individuals they represent. This nudging then moulds the residents over time to be better residents of the city, but it is done even more subtly than Foucauldian power was before. This subtlety is because the body of the individual is no longer the thing being targeted and controlled, but data doubles.

What is also interesting about this context is that power is not just acting on data doubles that represent the individual residents of the city; it is also acting on data doubles that represent the city, or at least parts of the city. While in some cases, the data doubles that power acts on are representations of individual residents, in other cases the collected data is used to make data doubles that represent the city itself. In Barcelona, the sensors used to measure the hydration levels of plants or to track empty car spaces are not collecting data to build a double that represents an individual, they are collecting data to build doubles that represent elements of the city's infrastructure. Just as data doubles can be constructed from individuals, they can also be constructed from elements of the city itself, such as infrastructures like the energy grid, systems like traffic lights and public transport, and even physical spaces such as parks or streets. These data doubles then represent fragments of the city in much the same way as data doubles built from data taken from individuals represent fragments of an individual. These "city data doubles" are useful subjects for the operation of power as they allow for the real-time manipulation of elements of the city itself. As these doubles are then targeted by exercises of power, residents of the city are nudged through the creation of choice architecture as the architecture of the city is manipulated around them.

Again, as with the other contexts considered in this chapter, the shift in the operation of Foucauldian power here presents major problems for accountability. Typically, exercises of Foucauldian power can be held to standards of accountability because we can assess the norms that individuals are being trained towards and how those individuals are being trained, and from there judge whether that is appropriate. That is, are those norms and the methods of training used in the exercise of power acceptable. By monitoring the acceptability of these exercises of power, and demanding the justification of any exercise of power, we can then enforce sanctions for abuses of power where those norms or methods are deemed not appropriate or acceptable in some way. However, this is undermined by the shift to the data double as the subject of power.

The use of data doubles in this context makes it difficult to monitor the appropriateness of exercises of power in this context, as the complex systems of the smart city can be manipulated in real time. Where in previous examples power is exercised on data doubles in response to predictions made using those doubles, in this context power is exercised both in response to and as part of the generation of predictions. Big data allows for multiple complex systems to be modelled and manipulated in real time, while monitoring the effects of those manipulations to adjust the exercising of power to more effectively achieve the goal of power. This enables a significant quantitative shift in the effectiveness of power in this context and makes it difficult to monitor the appropriateness of any given exercise of power, particularly from the perspective of the subject of power.

There are also only limited ways to enforce sanctions for any abuses of power, as the use of big data provides a near perfect façade of objectivity for the exercise of power. The operation of power in this context is positioned as a natural reaction to the objective facts of the world, rather than an attempt to manipulate and control the urban environment and thus the people who reside in that environment. As data about the city is aggregated and used to inform the decisions being made and choice architecture being constructed, these decisions are given an air of neutrality; of being reactive only to the objective data that has been collected. This is even more pronounced where the operation of the city is automated, such as where traffic lights are manipulated to redirect traffic by automated algorithms. Those being nudged by the city are being nudged by exercises of power that appear to be reasonable responses to the urban environment around them.

Finally, exercises of power in this context cannot be easily justified, if at all. As processes around the city are automated using big data, the training and nudging is black boxed, and as that happens it becomes harder to see how individuals are being nudged and trained towards the intended norms. Ultimately, this makes it difficult if not impossible to justify the operation of power. This is only compounded by power in this context acting on data doubles, especially data doubles of the city, as the operation of power becomes invisible to those individuals who are nudged towards acting in line with the norms set out by the agents of power.

Conclusion

These four contexts, namely the use of algorithmic risk assessment tools in criminal trials, predictive policing techniques, targeted advertising in political campaigns, and smart city infrastructure, are key examples of the ways in which power is impacted by the use of big data. Beyond this, they are also key examples of the kinds of decision-making processes that big data is increasingly being used for that we should be deeply concerned about. In each of these examples, there are hugely important decisions being made, such as who should be incarcerated, who should be subject to police surveillance and action, who gets to be in charge of government, and how our urban environments are designed and laid out. All these decisions are incredibly important, as they directly involve processes that can unfairly discriminate against people and limit their autonomy as well as determine how our society is structured and functions.

Furthermore, these contexts, and similar contexts, are excellent examples of the value of adopting a pluralistic attitude towards privacy as a supplement to the limitations of a privacy focused scheme of protections. While rights of privacy have been a more traditional framework for protecting individuals from the use of information to unfairly discriminate against them or undermine or limit their autonomy, in these four cases decisions are being made using information inferred through big data analytics in ways that do not breach traditional understandings of privacy. However, using a theoretical lens based on a pluralistic approach to power we can understand how these harms can occur with greater nuance by identifying the modes of power within a context in ways that can help us develop innovative and effective protections.

Chapter 8

Concluding Remarks

The rapid development and widespread usage of big data present us with urgent and significant ethical problems that must be addressed quickly. However, many of our existing ethical and legal protections, such as privacy, that we naturally reach for in response to the potential harms that can arise from the misuse of information are no longer adequate in the face of big data. I have argued in this thesis that we need a new approach. We need to, in a way, go back to basics and do important conceptual work by rethinking how we conceive of the concept of power and how big data can be used as a technology of power.

Conceptions of privacy have often been updated in response to new technological developments. Our current understanding of privacy is largely a response to the development of communications technologies over the mid-to-late 19th century (Igo 2018; Warren & Brandeis 1984), and work is being done to develop new accounts of privacy fit for the digital age such as contextual integrity, Floridi's informational privacy, and inferential privacy. However, big data presents a novel challenge to privacy-based approaches, because big data allows for information to move in ways that circumvent the protection of privacy. A minimal condition for the existence of a meaningful right to privacy is that we can identify and protect specific personal information, but big data undermines this assumption because of the *inference problem*. Many big data technologies can be used to infer sensitive personal information from otherwise unrelated information, and then use that information as part of decision-making processes. It is no longer possible to prevent the discovery of sensitive information, and more fundamentally the category of personal information is problematised. We still need privacy rights in a range of more traditional contexts, but the emergence of big data shows us the limitations of privacy rights. We must develop new legal and ethical tools instead to address these limitations.

While privacy protections are no longer the best tool when it comes to big data, harms inflicted on individuals through the misuse of information remain the primary ethical concern. Big data has changed the ways we use and discover information, but we are still using that information to make decisions and impact on people's lives. We need to take a step back and understand what impacts big data is having on the world, and how the use of big data affects people and social structures. As such, this thesis presents an alternative theoretical approach to a privacy focused one in analysing the new ways in which people are vulnerable to harm from the use of these new technologies, and this alternative theoretical approach is one based on an analysis of how big data can be used as a technology of power.

When examining the impact of big data on power, we must avoid falling into the trap of taking a one-size fits all approach. Those in the literature who also look at the relationship between big data and power, such as Cheney-Lippold (2011), Thompson (2016), Matzner (2017), Rouvroy (2016; 2013), Han (2017), Beer (2016), and Zuboff (2019), make the mistake of trying to set out a single unified theory of power that explains how power is changed by the use of big data. This is a mistake because not only is big data an umbrella term that refers to a wide collection of different technologies, power is also best understood as a kind of umbrella term that refers to a diverse range of phenomena. So, instead of asking simply "what is power in the age of big data?" to try and see how big data impacts on power, we should be inspired by Floridi's (2008b) level of abstraction methodology. We need to ask the right questions that will bring into focus the key features of a context and how big data is being used as a technology of power.

This is the central approach I have proposed in this thesis, whereby we work to identify the mode(s) of power present within a given context. The heart of this approach is a recognition that there are a wide range of ways in which big data technologies are used to enable and enhance the exercise of different kinds of power, and these applications exist over a similarly wide range of domains or contexts. To understand in each context how big data is used as part of power and in turn changes the operation of power, we must be sensitive to and focus in on the specific features of these contexts and the conceptual features of various theoretical accounts of power. Only then can we properly understand how power functions in that context, and how big data impacts on it. The questions I propose we ask are: "what is the intended outcome of power?", "who is exercising power?", "who is power exercised on?", and "how does this power function?". By answering these more specific questions, we can see the presence of different conceptual features of power, and in turn understand properly how power functions in that context.

The value of this approach, as demonstrated across this thesis through its practical application, is that it allows us to cut through both the hype and the doomsaying that surrounds big data, and to see with more nuance the impacts of big data on power within specific contexts. We should resist a view of big data as causing a kind of epochal shift, characterised by an entirely new kind of "big data power". A pluralistic attitude towards power and the asking of focused questions to identify different modes of power allows us to do this. Using the approach in this thesis, we can see that big data in many ways impacts on the operation of power much like any new technology, in that as it is used in the exercise of power it makes power more efficient, increases the range of power, or makes it more effective. These changes are important, but if we make the mistake of looking at big data in overly revolutionary terms, we may miss the fact that big data does not actually fundamentally change the nature of power, and that instead it is a series of tools that extend and expand the operation of power.

Where big data has led to a transformation in the exercise of power is through the emergence of a new subject of power, the *data double*. As decision-making processes are increasingly automated, the data double, fragmentary digital representations of a person that both contain and can be used to make predictions about a person, have emerged as a new subject of power. In some contexts, they are ideally suited for identifying people who are then targeted as subjects of power, while in others they replace people as the primary target of power. The modes of power approach in this thesis allows us to assess each context and determine whether power has begun to shift towards targeting data doubles, and if it is has what that means for the operation of power in that context.

While the focus of this thesis has been on describing how big data impacts on the world around us and how its use can harm individuals, the next step is to begin developing the necessary positive protections needed to replace rights to privacy. Given the complexity and the scale of the problem, as demonstrated in this thesis, multiple new strategies will be required to adequately protect individuals from harm. By identifying the different ways in which big data technologies can be used as a technology of power, we can develop different protections applicable to each context, in a multi-prong approach where necessary.

One possible strategy comes from the growing work on algorithmic accountability (Diakopoulos 2016; Garfinkel et al. 2017; Kroll et al. 2017), where the use of big data is made more accountable through measures aimed at increasing transparency around the development and implementation of algorithmic decision making. This may be through the development and adoption of ethical codes, the use of open-source coding for machine learning processes or developing processes by which individuals can appeal or challenge automated decisions more effectively.

Another possibility is to develop a new set of legal rights that relate to the ways in which individuals are represented by data doubles. These rights may confer upon individuals the right to know when a data double is constructed and used as part of the exercise of power as well as how that double was constructed, or rights to challenge the use of a data double or correct any erroneous data used in its creation. Rights of these kinds may help to reduce or avoid potential harms to individuals by limiting the extent to which data doubles become the subjects of power, and ensure that those people who will be impacted by an exercise of power can essentially stay in the loop.

A third possible approach is to set out new ethical and legal prescriptions on what kinds of power can be exercised in certain contexts. By setting out different modes of power, we can pinpoint with more accuracy than before the ways in which power functions in a context. This will then give us the ability to assess whether that mode of power should be morally permissible, i.e. should we be able to pursue that goal, should that agent have access to power, should that subject be targeted by power, should we allow power to function through those particular means? By answering these questions, we can begin to build up legal protections against the abuse of power tailored to each context.

Ultimately, the development of big data is in many ways like opening Pandora’s Box. These technologies have become globally ubiquitous. There is no realistic way to reverse the impact of big data, what we must do is ensure that we better understand the various impacts it has, in order to develop effective protections for people against the harms they may suffer from the use of big data. In this thesis, I have proposed a theoretical lens with which we can cut through the hype and the doomsaying, and that avoids falling into the traps of overgeneralising the many ways in which big data can be used as a technology of power. By adopting this lens, we can begin to properly understand the relationship between big data and power, the impacts that big data has on society, and what we can do going forward to prevent possible harms.

Bibliography

Ajunwa, I, Crawford, K & Ford, JS 2016, 'Health and big data: An ethical framework for health information collection by corporate wellness programs', *Journal of Law, Medicine & Ethics*, vol. 44, no. 3, pp. 474-80.

Amoore, L 2011, 'Data derivatives: On the emergence of a security risk calculus for our times', *Theory, Culture & Society*, vol. 28, no. 6, pp. 24-43.

Anderson, C 2008, *The end of theory: The data deluge makes the scientific method obsolete*, Wired, viewed 24 July 2018, <https://www.wired.com/2008/06/pb-theory/>.

Angwin, J, Larson, J, Mattu, S & Kirchner, L 2016, *Machine bias*, viewed 29 August 2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

APPR 2020, *How the PSA works*, Advancing Pretrial Policy & Research, viewed 27 July 2020, <https://advancingpretrial.org/psa/factors/>.

Arendt, H 1986, 'Communicative power', in S Lukes (ed.), *Power*, Basil Blackwell, Oxford, UK, pp. 59-74.

Arthur, C 2014, *Google flu trends is no longer good at predicting flu, scientists find*, The Guardian, viewed 2 August 2018, <https://www.theguardian.com/technology/2014/mar/27/google-flu-trends-predicting-flu>.

Asaro, PM 2019, 'AI ethics in predictive policing: From models of threat to an ethics of care', *IEEE Technology & Society Magazine*, vol. 38, no. 2, pp. 40-53.

Banking, S 2016, *Sesame credit: Data-driven credit scoring*, Fintech News Singapore, viewed 7 March 2019, <https://fintechnews.sg/1302/fintech/sesame-credit-data-driven-credit-scoring/>.

Barbaro, M 2019, *The Chinese surveillance state, part 1*, podcast, 6 May 2019, The Daily, viewed 16 July 2020, <https://www.nytimes.com/2019/05/06/podcasts/the-daily/china-surveillance-uighurs.html?>.

Barnes, B 1988, *The nature of power*, Polity Press, Oxford, Great Britain.

Barocas, S & Selbst, A 2014, *Losing out on employment because of big data mining*, The New York Times, viewed 19 February 2019, <https://www.nytimes.com/roomfordebate/2014/08/06/is-big-data-spreading-inequality/losing-out-on-employment-because-of-big-data-mining>.

Beer, D 2016, *Metric power*, Palgrave Macmillan UK, Basingstoke, UK.

Binder, C 2016, 'Happenings foreseen: Social media and the predictive policing of riots', *Sicherheit und Frieden (S+F)/Security and Peace*, vol. 34, no. 4, pp. 242-7.

Boerman, SC, Kruikemeier, S & Zuiderveen Borgesius, FJ 2017, 'Online behavioral advertising: A literature review and research agenda', *Journal of Advertising*, vol. 46, no. 3, pp. 363-76.

Botsman, R 2017, *Big data meets big brother as China moves to rate its citizens*, Wired, viewed 11 February 2019, <https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>.

boyd, d & Crawford, K 2012, 'Critical questions for big data', *Information, communication & society*, vol. 15, no. 5, pp. 662-79.

Bozdag, E 2013, 'Bias in algorithmic filtering and personalization', *Ethics and Information Technology*, vol. 15, no. 3, pp. 209-27.

Brey, P 2004, 'Ethical aspects of facial recognition systems in public places', *Journal of Information, Communication and Ethics in Society*, vol. 2, no. 2, pp. 97-109.

Brix, A 2020, 'Postal system - history', in *Encyclopedia Britannica*, Encyclopædia Britannica, <https://www.britannica.com/topic/postal-system/History>.

Burkell, JA 2016, 'Remembering me: Big data, individual identity, and the psychological necessity of forgetting', *Ethics and Information Technology*, vol. 18, no. 1, pp. 17-23.

Burrell, J 2016, 'How the machine 'thinks': Understanding opacity in machine learning algorithms', *Big Data & Society*, vol. 3, no. 1.

Calude, CS & Longo, G 2017, 'The deluge of spurious correlations in big data', *Foundations of Science*, vol. 22, no. 3, pp. 595-612.

Capurro, R 2008, 'On Floridi's metaphysical foundation of information ecology', *Ethics and Information Technology*, vol. 10, no. 2, pp. 167-73.

Carney, M 2018, *Leave no dark corner*, ABC News, viewed 14 March 2019, <https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278?nw=0>.

Charles, S 2020, *CPD decommissions 'strategic subject list'*, Chicago Sun Times, viewed 14 September 2020, <https://chicago.suntimes.com/city-hall/2020/1/27/21084030/chicago-police-strategic-subject-list-party-to-violence-inspector-general-joe-ferguson>.

Chen, M, Mao, S & Liu, Y 2014, 'Big data: A survey', *Mobile Networks and Applications*, vol. 19, no. 2, pp. 171-209.

Chen, QA & Mao, ZM 2018, *Connected cars can lie, posing a new threat to smart cities*, The Conversation, viewed 19 March 2019, <https://theconversation.com/connected-cars-can-lie-posing-a-new-threat-to-smart-cities-95339>.

Chen, S 2015, *How real estate uses big data to track clients*, Wall Street Journal, viewed 10 July 2017, <https://www.wsj.com/articles/how-real-estate-uses-big-data-to-track-clients-1431615728>.

Cheney-Lippold, J 2011, 'A new algorithmic identity: Soft biopolitics and the modulation of control', *Theory, Culture & Society*, vol. 28, no. 6, pp. 164-81.

Childress, S 2016, *The problem with "broken windows" policing*, PBS, viewed 14 February 2019, <https://www.pbs.org/wgbh/frontline/article/the-problem-with-broken-windows-policing/>.

Chorzempa, M, Triolo, P & Sacks, S 2018, *China's social credit system: A mark of progress or a threat to privacy?*, Peterson Institute for International Economics, viewed 7 July 2020, <https://www.piie.com/publications/policy-briefs/chinas-social-credit-system-mark-progress-or-threat-privacy>.

Clegg, S 1989, *Frameworks of power*, SAGE, Trowbride, Great Britain.

Cole, SA 2002, *Suspect identities : A history of fingerprinting and criminal identification*, Harvard University Press, Cambridge, US.

Coleman, N 2019, *Artificial intelligence can detect ptsd in your voice*, Futurism, viewed 26 April 2019, <https://futurism.com/artificial-intelligence-detect-ptsd-voice>.

Corbett-Davies, S, Pierson, E, Feller, A & Goel, S 2016, *A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear.*, The Washington Post, viewed 24 July 2018, <https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas/>.

Cunningham, L 2020, 'Roman catholicism', in *Encyclopedia Britannica*, Encyclopædia Britannica, <https://www.britannica.com/topic/Roman-Catholicism>.

Dahl, RA 1957, 'The concept of power', *Behavioral Science*, vol. 2, no. 3, pp. 201-15.

—— 1986, 'Power as the control of behavior', in S Lukes (ed.), *Power*, Basil Blackwell, Oxford, UK, pp. 37-58.

Deacon, R 2002, 'An analytics of power relations: Foucault on the history of discipline', *History of the Human Sciences*, vol. 15, no. 1, pp. 89-117.

Deanesly, M 1969, *A history of the medieval church : 590-1500*, 9th edn, Routledge, London, UK.

Degeling, M & Berendt, B 2018, 'What is wrong about robocops as consultants? A technology-centric critique of predictive policing', *AI & Society*, vol. 33, no. 3, pp. 347-56.

Del Valle, S 2019, *How big data can help save the world*, Scientific American, viewed 6 November 2020, <https://blogs.scientificamerican.com/observations/how-big-data-can-help-save-the-world/>.

Deleuze, G 1992, 'Postscript on the societies of control', *October*, vol. 59, pp. 3-7.

DeMichele, M, Baumgartner, P, Wenger, M, Barrick, K & Comfort, M 2020, 'Public safety assessment', *Criminology & Public Policy*, vol. 19, no. 2, pp. 409-31.

Diakopoulos, N 2016, 'Accountability in algorithmic decision making', *Communications of the ACM*, vol. 59, no. 2, pp. 56-62.

Dimick, P 2016, *How to use big data to enhance employee performance*, Datafloq, viewed 15 February 2019, <https://datafloq.com/read/how-to-use-big-data-enhance-employee-performance/1937>.

Dormehl, L 2019, *Amazing app promises a full fitness checkup from a 30-second selfie* DigitalTrends, viewed 15 August 2019, <https://www.digitaltrends.com/cool-tech/university-of-toronto-selfie-health-app/>.

Doyle, T 2010, 'A critique of information ethics', *Knowledge, Technology & Policy*, vol. 23, no. 1, pp. 163-75.

Duff-Brown, B 2020, *How Taiwan used big data, transparency and a central command to protect its people from coronavirus*, Stanford University, viewed 18 July 2020, <https://fsi.stanford.edu/news/how-taiwan-used-big-data-transparency-central-command-protect-its-people-coronavirus>.

Eagleton, H 2019, *Leveraging big data to boost employee performance*, Innovation Enterprise Channels, viewed 15 February 2019, <https://channels.theinnovationenterprise.com/articles/leveraging-big-data-to-boost-employee-performance>.

Ess, C 2008, 'Luciano Floridi's philosophy of information and information ethics: Critical reflections and the state of the art', *Ethics and Information Technology*, vol. 10, no. 2, pp. 89-96.

Falgoust, M 2016, 'Data science and designing for privacy', *Techné: Research in Philosophy and Technology*, vol. 20, no. 1, pp. 51-68.

Fido, M & Skinner, K 1999, *The official encyclopedia of Scotland Yard*, Virgin Books, London, UK.

First, D 2018, 'Will big data algorithms dismantle the foundations of liberalism?: How the emergence of recommendation algorithms will shape the pursuit of happiness in the 21st century', *AI and Society*, vol. 33, no. 4, pp. 545-56.

Fisher, T 2020, *Terabytes, gigabytes, & petabytes: How big are they?*, Lifewire, viewed 10 October 2020, <https://www.lifewire.com/terabytes-gigabytes-amp-petabytes-how-big-are-they-4125169>.

Fitzpatrick, J & DeSalvo, K 2020, *Community mobility reports*, Google, viewed 18 July 2020, <https://www.blog.google/technology/health/covid-19-community-mobility-reports?hl=en>.

Floridi, L 1999, 'Information ethics: On the philosophical foundation of computer ethics', *Ethics and Information Technology*, vol. 1, no. 1, pp. 33-52.

—— 2002, 'On the intrinsic value of information objects and the infosphere', *Ethics and Information Technology*, vol. 4, no. 4, pp. 287-304.

—— 2005, 'The ontological interpretation of informational privacy', *Ethics & Information Technology*, vol. 7, no. 4, pp. 185-200.

—— 2006, 'Four challenges for a theory of informational privacy', *Ethics and Information Technology*, vol. 8, no. 3, pp. 109-19.

—— 2008a, 'Information ethics: A reappraisal', *Ethics and Information Technology*, vol. 10, no. 2, pp. 189-204.

—— 2008b, 'The method of levels of abstraction', *Minds & Machines*, vol. 18, no. 3, pp. 303-29.

—— 2014a, *The 4th revolution: How the infosphere is reshaping human reality*, Oxford University Press, Oxford, UK.

—— 2014b, 'Open data, data protection, and group privacy', *Philosophy & Technology*, vol. 27, no. 1, pp. 1-3.

—— 2016, 'Group privacy: A defence and an interpretation.' In Taylor, L, Floridi, L & van der Sloot, B (eds.) *Group Privacy*, Springer, Cham, pp. 83-100.

Foucault, M 1988, *The history of sexuality, vol. 1: An introduction*, trans. R Hurley, Vintage Books, New York, US.

—— 1995, *Discipline and punish: The birth of the prison*, trans. A Sheridan, Vintage Books, New York, US.

Gage, D 2014, *Big data uncovers some weird correlations*, Wall Street Journal, viewed 20 February 2018, <https://www.wsj.com/articles/SB10001424052702303369904579423132072969654>.

Gallie, W. B. 1956, 'IX.-Essentially Contested Concepts.', *Proceedings of the Aristotelian Society*, vol. 56, no. 1, pp. 167-198.

Galbraith, JK 1984, *The anatomy of power*, Hamis Hamilton Ltd, London, UK.

García-Hodges, A, Sottile, C & Ward, J 2020, *Man wrongfully arrested due to facial recognition software talks about 'humiliating' experience*, NBC News, viewed 22 July 2020, <https://www.nbcnews.com/business/business-news/man-wrongfully-arrested-due-facial-recognition-software-talks-about-humiliating-n1232184>.

Garfinkel, S, Matthews, J, Shapiro, SS & Smith, JM 2017, 'Toward algorithmic transparency and accountability', *Communications of the ACM*, vol. 60, no. 9, pp. 5-.

Gascó-Hernandez, M 2018, 'Building a smart city: Lessons from barcelona', *Communications of the ACM*, vol. 61, no. 4, pp. 50-7.

Gorner, J & Sweeney, A 2020, *For years chicago police rated the risk of tens of thousands being caught up in violence. That controversial effort has quietly been ended.*, Chicago Tribune, viewed 15 July 2020, <https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html>.

Grassegger, H & Krogerus, M 2017, *The data that turned the world upside down*, VICE, viewed 25 February 2019, <https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win>.

Green, B 2020, 'The false promise of risk assessments: Epistemic reform and the limites of fairness', in *Conference on Fairness, Accountability, and Transparency*, Barcelona, Spain, pp. 594-606.

Green, J & Issenberg, S 2016, *Inside the Trump bunker, with days to go*, Bloomberg, viewed 16 April 2019, <https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go>.

Griffard, M 2019, 'A bias-free predictive policing tool?: An evaluation of the NYPD's patternizr', *Fordham Urban Law Journal*, vol. 47, no. 1, pp. 43-83.

Haggerty, KD & Ericson, RV 2000, 'The surveillant assemblage', *British Journal of Sociology*, vol. 51, no. 4, pp. 605-22.

Hamilton, IA 2020, *The UK and Australia are investigating clearview AI, the facial recognition firm that scraped billions of photos from social media*, Business Insider Australia, viewed 13 July 2020, <https://www.businessinsider.com.au/clearview-ai-under-investigation-in-the-uk-and-australia-

2020-7>.

Hamilton, IA & Cain, Á 2019, *Amazon warehouse employees speak out about the 'brutal' reality of working during the holidays, when 60-hour weeks are mandatory and ambulance calls are common*, Business Insider, viewed 18 March 2019, <https://www.businessinsider.com/amazon-employees-describe-peak-2019-2?r=AU&IR=T>.

Han, B-C 2017, *Psychopolitics: Neoliberalism and new technologies of power*, trans. E Butler, Verso, London, UK.

Herz, P 2007, 'Finances and costs of the Roman army', in P Erdkamp (ed.), *A companion to the Roman army*, Wiley-Blackwell, Oxford, UK, pp. 306-22.

Hill, K 2020, *The secretive company that might end privacy as we know it*, New York Times, viewed 17 July 2020, <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

Hobbes, T 1839, *The English works of Thomas Hobbes of Malmesbury*, vol. 1, 11 vols., W Molesworth (ed.), J. Bohn.

—— 2018, *Leviathan*, First Avenue Editions, Minneapolis, US.

Holmes, B 2017, *For a flavor boost, chefs turn to big data*, Wall Street Journal, viewed 10 July 2017, <https://www.wsj.com/articles/for-a-flavor-boost-chefs-turn-to-big-data-1490369287>.

Horowitz, J 2020, *Tech companies are still helping police scan your face*, CNN, viewed 21 July 2020, <https://edition.cnn.com/2020/07/03/tech/facial-recognition-police/index.html>.

HRD 2018, *How dell is using big data to engage employees*, HRD, viewed 19 February 2019, <https://www.hcamag.com/au/specialisation/hr-technology/how-dell-is-using-big-data-to-engage-employees/151933>.

Huang, Z 2017, *I fixed my poor credit score by being a more loyal alibaba consumer*, Quartz, viewed 1 June 2018, <https://qz.com/1097766/i-fixed-my-poor-sesame-credit-score-by-being-a-more-loyal-user-of-alibabas-wallet-app-alipay-in-china/>.

Hughes, M 2019, *Bots drove nearly 40% of internet traffic last year — and the naughty ones are getting smarter*, TheNextWeb, viewed 30 August 2020, <https://thenextweb.com/security/2019/04/17/bots-drove-nearly-40-of-internet-traffic-last-year-and-the-naughty-ones-are-getting-smarter/>.

Hull, G, Lipford, HR & Latulipe, C 2010, 'Contextual gaps: Privacy issues on Facebook', *Ethics and Information Technology*, vol. 13, no. 4, pp. 289-302.

Hvistendahl, M 2016, *Can 'predictive policing' prevent crime before it happens?*, ScienceMag, viewed 23 September 2020, <https://www.sciencemag.org/news/2016/09/can-predictive-policing-prevent-crime-it-happens>.

Igo, S 2018, *The known citizen: A history of privacy in modern America*, Harvard University Press, Cambridge, US.

Jiang, X 2015, 'Fingerprint classification', in *Encyclopedia of Biometrics*, AJ Stan Li (ed.), 2nd edn, Springer Reference, New York, US.

Jin, K & McGorman, L 2020, *Data for good: New tools to help health researchers track and combat covid-19*, Facebook, viewed 18 July 2020, <https://about.fb.com/news/2020/04/data-for-good/>.

John Berry, DS 2001, 'History and development of fingerprinting', in RG Henry Lee (ed.), *Advances in fingerprint technology*, 2nd edn, CRC Press, pp. 14-53.

Johnson, B 2010, *Privacy no longer a social norm, says Facebook founder*, The Guardian, viewed 21 July 2020, <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>.

Kantor, J & Streitfeld, D 2015, *Inside Amazon: Wrestling big ideas in a bruising workplace*, New York Times, viewed 15 February 2019, <https://www.nytimes.com/2015/08/16/technology/inside-amazon-wrestling-big-ideas-in-a-bruising-workplace.html>.

Kim, TW & Werbach, K 2016, 'More than just a game: Ethical issues in gamification', *Ethics and Information Technology*, vol. 18, no. 2, pp. 157-73.

Kirkpatrick, G 2008, *Technology and social power*, Palgrave Macmillan.

Kirkpatrick, K 2017, 'It's not the algorithm, it's the data', *Communications of the ACM*, vol. 60, no. 2, pp. 21-3.

Kitchin, R 2014, *Data revolution: Big data, open data, data infrastructures and their consequences*, Sage Publications, Croydon, UK.

—— 2014b, 'The real-time city? Big data and smart urbanism', *GeoJournal*, vol. 79, no. 1, pp. 1-14.

Koetse, M 2018, *Baihang and the eight personal credit programmes: A credit leap forward*, What's On Weibo, viewed 14 March 2019, <https://www.whatsonweibo.com/baihang-and-the-eight-personal-credit-programmes-a-credit-leap-forward/>.

Kolb, A 2001, 'Transport and communication in the Roman state: The cursus publicus', in C Adams & R Laurence (eds), *Travel and geography in the Roman empire*, Routledge, London, pp. 95-105.

Kosinski, M, Stillwell, D & Graepel, T 2013, ‘Private traits and attributes are predictable from digital records of human behavior’, *Proceedings of the National Academy of Sciences of the United States of America*, vol. 110, no. 15, pp. 5802-5.

Kroll, JA, Huey, J, Barocas, S, Felten, EW, Reidenberg, JR, Robinson, DG & Yu, H 2017, ‘Accountable algorithms’, *University of Pennsylvania Law Review*, vol. 165, no. 3, pp. 633-705.

Kubler, K 2017, ‘State of urgency: Surveillance, power, and algorithms in france’s state of emergency’, *Big Data & Society*, vol. 4, no. 2.

Kunichoff, Y & Sier, P 2017, *The contradictions of chicago police’s secretive list*, Chicago Mag, viewed 14 September 2020, <https://www.chicagomag.com/city-life/August-2017/Chicago-Police-Strategic-Subject-List/>.

Laney, D 2001, ‘3d data management: Controlling data volume, velocity and variety’, *META Group Research Note*, vol. 6, p. 70.

Lazer, D, Kennedy, R, King, G & Vespignani, A 2014, ‘The parable of google flu: Traps in big data analysis’, *Science*, vol. 343, no. 6176, pp. 1203-5.

Lee-Morrison, L 2018, ‘A portrait of facial recognition: Tracing a history of a statistical way of seeing’, *Philosophy of Photography*, vol. 9, no. 2, pp. 107-30.

Leeuwen, J 2014, ‘On Floridi’s method of levels of abstraction’, *Minds & Machines*, vol. 24, no. 1, pp. 5-17.

Lewis, P 2017, *‘Our minds can be hijacked’: The tech insiders who fear a smartphone dystopia*, The Guardian, viewed 6 November 2020, <https://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia>.

Liao, S 2018, *Amazon warehouse workers skip bathroom breaks to keep their jobs, says report*, The Verge, viewed 19 March 2019, <https://www.theverge.com/2018/4/16/17243026/amazon-warehouse-jobs-worker-conditions-bathroom-breaks>.

Loi, M & Christen, M 2019, ‘Two concepts of group privacy’, *Philosophy & Technology*, vol. 33, pp. 207-224.

Lukes, S (ed.) 1986, *Power*, Basil Blackwell, Oxford, UK.

—— 2005, *Power: A radical view*, 2nd edn, Palgrave Macmillan, Ebbw Vale, Great Britain.

Lyon, D 2007, *Surveillance studies: An overview*, Polity, Cornwall, Great Britain.

Mai, JE 2016, ‘Personal information as communicative acts’, *Ethics and Information Technology*, vol. 18, no. 1, pp. 51-7.

Mann, M & Smith, M 2017, ‘Automated facial recognition technology: Recent developments and approaches to oversight’, *University of New South Wales Law Journal*, vol. 40, no. 1, pp. 121-45.

Marr, B 2018, *5 inspiring ways organizations are using HR data*, Forbes, viewed 19 February 2019, <https://www.forbes.com/sites/bernardmarr/2018/05/11/5-inspiring-ways-organizations-are-using-hr-data/#3b69c2461872>.

Martinich, AP & Hoekstra, K 2016, *The Oxford handbook of Hobbes*, Oxford University Press, UK.

Matzner, T 2014, ‘Why privacy is not enough privacy in the context of “ubiquitous computing” and “big data”’, *Journal of Information, Communication and Ethics in Society*, vol. 12, no. 2, pp. 93-106.

—— 2017, ‘Opening black boxes is not enough – data-based surveillance in discipline and punish and today’, *Foucault Studies*, no. 23, pp. 27-45.

Mayer-Schönberger, V & Cukier, K 2013, *Big data : A revolution that will transform how we live, work, and think*, Houghton Mifflin Harcourt, Boston, US.

Meredith, S 2018, *Facebook-cambridge analytica: A timeline of the data hijacking scandal*, CNBC, viewed 25 February 2019, <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>.

Metz, R 2018, *This company embeds microchips in its employees, and they love it*, MIT Technology Review, viewed 19 March 2019, <https://www.technologyreview.com/2018/08/17/140994/this-company-embeds-microchips-in-its-employees-and-they-love-it/>.

—— 2020, *Going back to work or school? An algorithm may warn you to keep your distance from others*, CNN Business, viewed 29 July 2020, <https://edition.cnn.com/2020/07/28/tech/ai-social-distancing-in-offices-and-schools/index.html>.

Miller, A 2018, *More companies are using technology to monitor employees, sparking privacy concerns*, ABC News, viewed 19 February 2019, <https://abcnews.go.com/US/companies-technology-monitor-employees-sparking-privacy-concerns/story?id=53388270>.

Mittelstadt, B & Floridi, L 2016, ‘The ethics of big data: Current and foreseeable issues in biomedical contexts’, *Science & Engineering Ethics*, vol. 22, no. 2, pp. 303-41.

Mittelstadt, B 2017, ‘From individual to group privacy in big data analytics’, *Philosophy & Technology*, vol. 30, no. 4, pp. 475-494.

Moor, JH 1997, ‘Towards a theory of privacy in the information age’, *Computers & Society*, vol. 27, no. 3, pp. 27-32.

Morriss, P 1987, *Power: A philosophical analysis*, St. Martin’s Press, New York, US.

Moser, S 2013, *New cities: Opportunities, visions and challenges cityquest – KAEC forum 2013: Summary and analysis report*, New Cities Foundation <bit.ly/CityquestReport2013>.

Naughton, J 2016, *Death by drone strike, dished out by algorithm*, The Guardian, viewed 27 March 2017, <https://www.theguardian.com/commentisfree/2016/feb/21/death-from-above-nia-csa-skynet-algorithm-drones-pakistan>.

Neidhart, C 2018, *Welcome to Songdo, South Korea: The smartest of smart cities*, Worldcrunch, viewed 18 June 2019, <https://worldcrunch.com/smarter-cities-1/welcome-to-songdo-south-korea-the-smartest-of-smart-cities>.

Nickelsburg, M 2020, *Amazon tops 935k employees as of this week, as pandemic-driven hiring spree continues*, GeekWire, viewed 14 July 2020, <https://www.geekwire.com/2020/amazon-tops-935k-employees-week-pandemic-driven-hiring-spree-continues/>.

Nikei Asian Review 2016, *Japan banks unleashing AI marketing tech*, Nikkei Asian Review, viewed 26 February 2018, <https://asia.nikkei.com/Business/Companies/Japan-banks-unleashing-AI-marketing-tech>.

Nissenbaum, H 2004, ‘Privacy as contextual integrity’, *Washington law review*, vol. 79, no. 1, pp. 119-57.

—— 2010, *Privacy in context: Technology, policy, and the integrity of social life*, Stanford Law Books, California, US.

—— 2011, ‘A contextual approach to privacy online’, *Daedalus*, vol. 140, no. 4, pp. 32-48.

—— 2018, ‘Respecting context to protect privacy: Why meaning matters’, *Science and Engineering Ethics*, vol. 24, pp. 831-52.

O’Neil, C 2016, *Weapons of math destruction : How big data increases inequality and threatens democracy*, New York Crown Publishers, New York, US.

Ohm, P 2009, ‘Broken promises of privacy: Responding to the surprising failure of anonymization’, *UCLA Law Review*, vol. 57, p. 1701.

Parsons, T 1986, ‘Power and the social system’, in S Lukes (ed.), *Power*, Basil Blackwell, Oxford, UK, pp. 94-143.

Perryer, C, Celestine, NA, Scott-Ladd, B & Leighton, C 2016, ‘Enhancing workplace motivation through gamification: Transferrable lessons from pedagogy’, *International Journal of Management Education*, vol. 14, no. 3, pp. 327-35.

Picon, A 2015, *Smart cities*, John Wiley & Sons, Italy.

Pillania, R 2018, *Decoding the smart city concept*, Entrepeneur India, viewed 19 March 2019, <https://www.entrepreneur.com/article/315975>.

Popper, KR 2002, *The logic of scientific discovery*, Routledge, London, UK.

Power, A 2016, *Under watchful eyes*, Lapham’s Quarterly, viewed 24 January 2020, <https://www.laphamsquarterly.org/spies/under-watchful-eyes>.

Precious, K 2020, *Can you predict customer’s loan default using machine learning?*, Medium, viewed 7 August 2020, <https://medium.com/datadriveninvestor/can-you-predict-customers-loan-default-using-machine-learning-be774489b8f5>.

Rachels, J 1975, ‘Why privacy is important’, *Philosophy & Public Affairs*, vol. 4, no. 4, pp. 323-33.

Raphael, R & Xi, L 2019, *Discipline and punish: The birth of China’s social-credit system*, The Nation, viewed 6 July 2020, <https://www.thenation.com/article/archive/china-social-credit-system/>.

Ricken, N 2006, ‘The power of power – questions to Michel Foucault’, *Educational Philosophy and Theory*, vol. 38, no. 4, pp. 541-60.

Ricker, T 2019, *The US, like China, has about one surveillance camera for every four people, says report*, The Verge, viewed 16 July 2020, <https://www.theverge.com/2019/12/9/21002515/surveillance-cameras-globally-us-china-amount-citizens>.

Robbins, M 2016, ‘Has a rampaging AI algorithm really killed thousands in Pakistan?’, *The Guardian*, 19 February, <https://www.theguardian.com/science/the-lay-scientist/2016/feb/18/has-a-rampaging-ai-algorithm-really-killed-thousands-in-pakistan>.

Rouvroy, A 2016, ‘Algorithmic governmentality: Radicalisation and immune strategy of capitalism and neoliberalism?’, *La Deleuziana*, no. 3, pp. 30-6.

Rouvroy, A & Berns, T 2013, ‘Algorithmic governmentality and prospects of emancipation. Disparateness as a precondition for individuation through relationships?’, *Réseaux*, vol. 177, no. 1, pp. 163-96.

Sattarov, F 2019, *Power and technology: A philosophical and ethical analysis*, Rowman & Littlefield International, London, UK.

Sax, M 2016, 'Big data: Finders keepers, losers weepers?', *Ethics and Information Technology*, vol. 18, no. 1, pp. 25-31.

Schedler, A 1999, 'Conceptualizing accountability', in A Schedler, LJ Diamond & MF Plattner (eds), *The self-restraining state: Power and accountability in new democracies*, Lynne Rienner Publishers, Boulder, US, pp. 13-28.

Scheidel, W & Meeks, E 2012, *Orbis: The Stanford geospatial network model of the Roman world*, Stanford University, viewed 24 January 2020, <http://orbis.stanford.edu/>.

Schirato, T, Danaher, J & Webb, J (eds) 2012, *Understanding Foucault: A critical introduction*, 2nd edn, Allen & Unwin, Crows Nest, Australia.

Shapiro, A 2017, 'Reform predictive policing', *Nature*, vol. 541, no. 7638, pp. 458-60.

Silver, E & Chow-Martin, L 2002, 'A multiple models approach to assessing recidivism risk: Implications for judicial decision making', *Criminal Justice and Behavior*, vol. 29, no. 5, pp. 538-68.

Singer, N & Metz, C 2019, *Many facial-recognition systems are biased, says U.S. Study*, The New York Times, viewed 21 August 2020, <https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html>.

Smith, M 2016, *In Wisconsin, a backlash against using data to foretell defendants' futures*, The New York Times, viewed 19 March 2019, <https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html>.

Solon, O 2018, *Amazon patents wristband that tracks warehouse workers' movements*, The Guardian, viewed 19 February 2019, <https://www.theguardian.com/technology/2018/jan/31/amazon-warehouse-wristband-tracking>.

Solove, DJ 2011, *Nothing to hide: The false tradeoff between privacy and security*, Yale University Press, New Haven, US.

Song, V 2019, *Microsoft quietly pulls its database of 100,000 faces used by Chinese surveillance companies*, Gizmodo, viewed 16 July 2020, <https://www.gizmodo.com.au/2019/06/microsoft-quietly-pulls-its-database-of-100000-faces-used-by-chinese-surveillance-companies/>.

Stevenson, M 2018, 'Assessing risk assessment in action', *Minnesota Law Review*, vol. 103, no. 1, pp. 303-84.

Stilgoe, J 2018, 'Machine learning, social learning and the governance of self-driving cars', *Social Studies of Science*, vol. 48, no. 1, pp. 25-56.

Sun, B 2020, *China's social credit system: Western perceptions vs. reality*, The Startup, viewed 3 July 2020, <https://medium.com/swlh/chinas-social-credit-system-western-perceptions-vs-reality-7162b30423b8>.

Taagepera, R 1978, 'Size and duration of empires: Systematics of size', *Social science research*, vol. 7, no. 2, pp. 108-27.

Tangermann, V 2019, *Amazon used an AI to automatically fire low-productivity workers*, Futurism, viewed 16 July 2020, <https://futurism.com/amazon-ai-fire-workers>.

Tavani, HT 2007, 'Philosophical theories of privacy: Implications for an adequate online privacy policy', *Metaphilosophy*, vol. 38, no. 1, pp. 1-22.

—— 2008a, 'Floridi's ontological theory of informational privacy: Some implications and challenges', *Ethics and Information Technology*, vol. 10, no. 2, pp. 155-66.

—— 2008b, 'Informational privacy: Concepts, theories, and controversies', in KE Himma & HT Tavani (eds), *The handbook of information and computer ethics*, Wiley, Hoboken, New Jersey, pp. 131-64.

Tavani, HT & Moor, JH 2001, 'Privacy protection, control of information, and privacy-enhancing technologies', *Computers & Society*, vol. 31, no. 1, pp. 6-11.

Taylor, L, Floridi, L & van der Sloot, B 2016, 'Introduction: A New Perspective on Privacy', in Taylor, L, Floridi, L & van der Sloot, B (eds.) *Group Privacy*, Springer, Cham, pp. 1-12

Thaler, RH & Sunstein, CR 2008, *Nudge: Improving decisions about health, wealth, and happiness*, Yale University Press, New Haven, US.

The Sentencing Project 2018, *Report of the sentencing project to the United Nations special rapporteur on contemporary forms of racism, racial discrimination, xenophobia, and related intolerance*, The Sentencing Project, Washington, D.C. <https://www.sentencingproject.org/publications/un-report-on-racial-disparities/>.

Thompson, G 2016, 'Computer adaptive testing, big data and algorithmic approaches to education', *British Journal of Sociology of Education*, vol. 38, no. 6, pp. 827-40.

Tieman, R 2017, *Barcelona: Smart city revolution in progress*, Financial Times, viewed 19 March 2019, <https://www.ft.com/content/6d2fe2a8-722c-11e7-93ff-99f383b09ff9>.

Timmer, J 2014, *Researchers warn against the rise of "big data hubris"*, Ars Technica, viewed 2 August 2018, <https://arstechnica.com/science/2014/03/researchers-warn-against-the-rise-of-big-data-

hubris/>.

Turner, K 2016, *Are performance-monitoring wearables an affront to workers' rights?*, The Switch, viewed 19 March 2019, <https://www.washingtonpost.com/news/the-switch/wp/2016/08/05/are-performance-monitoring-wearables-an-affront-to-workers-rights/>.

van Dijck, J 2014, 'Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology', *Surveillance & Society*, vol. 12, no. 2, pp. 197-208.

van Rijmenam, M 2019, *How big data can help save the earth*, Medium, viewed 6 November 2020, <https://medium.com/@markvanrijmenam/how-big-data-can-help-save-the-earth-9767dd078508>.

Vincent, D 2016, *Privacy: A short history*, Polity Press, Cambridge, UK.

Wachter, S & Mittelstadt, B 2019, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI', *Columbia Business Law Review*, vol. 2019, no. 2, pp. 494-620.

Warren, S & Brandeis, L 1984, 'The right to privacy [the implicit made explicit]', in FD Schoeman (ed.), *Philosophical dimensions of privacy: An anthology*, Cambridge University Press, USA, pp. 75-103.

Watershed 2019, *Playable city*, Watershed, viewed 19 March 2019, <https://www.playablecity.com/>.

Weber, M, Wittich, C & Roth, G (eds) 1978, *Economy and society: An outline of interpretive sociology*, vol. 1, University of California Press, Berkeley, California.

Westin, A 1984, 'The origins of modern claims to privacy', in FD Schoeman (ed.), *Philosophical dimensions of privacy: An anthology*, Cambridge University Press, USA, pp. 56-74.

WHO 2020, *Timeline of who's response to covid-19*, World Health Organization, viewed 17 July 2020, <https://www.who.int/news-room/detail/29-06-2020-covidtimeline>.

Wiggers, K 2020, *Density raises $51 million to promote social distancing with AI occupancy-tracking sensors*, Venture Beat, viewed 29 July 2020, <https://venturebeat.com/2020/07/28/density-raises-51-million-to-promote-social-distancing-with-ai-occupancy-tracking-sensors/>.

Williams, CA 2003, 'Police surveillance and the emergence of CCTV in the 1960s', *Crime Prevention and Community Safety*, vol. 5, no. 3, pp. 27-37.

Willis, KS & Aurigi, A 2018, *Digital and smart cities*, Routledge, New York, US.

Wong, J 2020, *Countries are using apps and data networks to keep tabs on the pandemic*, The Economist, viewed 18 July 2020, <https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic>.

Wood, DM & Mackinnon, D 2019, 'Partial platforms and oligoptic surveillance in the smart city', *Surveillance & Society*, vol. 17, no. 1/2, pp. 176-82.

Wood, S 2017, *What that Facebook quiz is doing to your privacy*, The Sydney Morning Herald, viewed 6 February 2018, <https://www.smh.com.au/lifestyle/what-that-facebook-quiz-is-doing-to-your-privacy-20170706-gx5zvj.html>.

World Health Organization 2020, *Covid-19 weekly epidemiological update - 15 december 2020*, World Health Organization, viewed 21 December 2020, <file:///C:/Users/New/AppData/Local/Temp/20201215_Weekly_Epi_Update_18.pdf>.

Wright, E 2018, *The smart infrastructure that will save us from our dumb cities*, Wired, viewed 19 March 2019, <https://www.wired.co.uk/article/building-the-megacities-of-the-future>.

Xu, VX & Xiao, B 2018, *China's social credit system seeks to assign citizens scores, engineer social behaviour*, ABC News, viewed 1 June 2018, <https://www.abc.net.au/news/2018-03-31/chinas-social-credit-system-punishes-untrustworthy-citizens/9596204>.

Yeates, C 2017, *How big data can keep the banks in check*, The Sydney Morning Herald, viewed 8 February 2018, <https://www.smh.com.au/opinion/how-big-data-can-keep-the-banks-in-check-20170116-gts1s8.html>.

Yeginsu, C 2018, *If workers slack off, the wristband will know. (and Amazon has a patent for it.)*, The New York Times, viewed 19 February 2019, <https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html>.

You, T 2018, *Millions in China have been banned from travelling after being deemed 'untrustworthy' by social credit system*, Daily Mail Australia, viewed 1 June 2018, <https://www.dailymail.co.uk/news/article-5757815/Millions-people-China-banned-travelling-social-credit-system.html>.

Yuan, S 2020, *How China is using AI and big data to fight the coronavirus*, Al Jazeera, viewed 18 July 2020, <https://www.aljazeera.com/news/2020/03/china-ai-big-data-combat-coronavirus-outbreak-200301063901951.html>.

Yue, H & Yingzhe, G 2020, *Tencent launches sesame credit competitor*, Caixin, viewed 3 July 2020, <https://www.caixinglobal.com/2020-06-08/tencent-launches-sesame-credit-competitor-101564601.html>.

Zhou, X, Liang, H & Dong, Z 2017, ‘A personalized recommendation model for online apparel shopping based on Kansei engineering’, *International Journal of Clothing Science and Technology*, vol. 29, no. 1, pp. 2-13.

Zuboff, S 2019, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, Public Affairs, New York, US.