Spring 2022

Comparing Political Implications of Punitive Paradigms in Digital Surveillance and Data Driven Algorithms between the Polities of the United States of America and the People's Republic of China

Shedelande Lily Carpenter
Bard College

Comparing Political Implications of Punitive Paradigms in Digital Surveillance and Data Driven Algorithms between the Polities of the United States of America and the People's Republic of China

Senior Project Submitted to

The Division of Social Studies

of Bard College

by

Shedelande Carpenter

Annandale-on-Hudson, New York

May, 4 2022

Dedication

This project would not have been possible without the unwavering support of my parents who have invested in my education and believed in me every step of the way. I dedicate this project to you, my eternal cheerleaders!

Acknowledgements

Table of Contents

Introduction……..1
Chapter 1……..5
Chapter 2……21
Chapter 3……47
Conclusion…….66
Bibliography……...67

Introduction

The critical questions and anxieties surrounding the encroachment of data driven algorithmic technology is not unprecedented. Most technological advancements throughout history have been met with some sort of resistance that eventually wanes with general acceptance of the technologies' expediency. Convenience and practicality do not need to be sacrificed to develop a more critical and comprehensive approach to digital surveillance, but rather supplemented with an equitable, conscientious long term model. I analyze the far reaching political implications of these new modes of technocratic management through the abolitionist lens. Crime has long been analyzed as a way to further understand underlying social problems in civil society and policing and prisons are the most prominent and well funded solution for managing these instances of unrest. Abolitionist organizing seeks to redirect resources from the penal system to invest in education, health services, and employment to address the roots of crime ultimately divesting from carceral or punitive mechanisms of justice and correctional institutions. The Abolitionist framework is the concentration on policing as an institution through which many forms of oppression intersect and are legitimized through structural and violent reinforcement. The essential element to this praxis is tenacious imagination or radical exploration coupled with conscientious scrutiny over the distribution of material resources to center and empower the most vulnerable populations under a socioeconomic hierarchy. It follows the conflict theory model of Marxists with the premise that police exist as a tool for the bourgeoisie to violently enforce class stratification and protect their property. Abolitionists add to this model with a crucial emphasis on intersectionality: how race, class, gender, disability and other marginal identities interact with the system to exacerbate the impact of capitalist

domination. Through an intersectional approach to the abolition of policing, other forms of systemic oppression can be understood and dismantled. To the extent abolitionism helps understand mechanisms of repression that develop from policing, it is also a useful lens for understanding the broader societal consequences that stem from implementation of digital surveillance or algorithms into this nexus of crime and punishment. The fear surrounding this technology is rational and legitimate, however crises concerning personal privacy and inequality are not inherent to the development of algorithms, but rather the society that produces them. The technology itself is neutral; alone, it does not have the agency to oppress or liberate a population, yet it is still central to questions about power and exploitation. For example, an algorithm designed to recognize names of people, process, then categorize them is neutral. How it categorizes the names and the meaning attached to those categorizations, however, cannot be neutral as it is informed by human subjectivity. Unfortunately, data driven algorithmic technology is implemented with the misleading assumption that it removes human subjectivity for a more mathematical, statistical, and colorblind approach to civil management. Helga Nowotny refers to the work of scholars of science and technology studies (STS) who find that:

> Technologies are always selectively taken up. They are gendered. They are appropriated and translated into products around which new markets emerge that give another boost to global capitalism. The benefits of technological innovation are never equally distributed, and already existing social inequalities are deepened through accelerated technological change. But it is never technology alone that acts as an external force bringing about social change. Rather, technologies and technological change are products and the outcome of societal, cultural and economic conditions and result from many co-productive processes (2021).

If technology exists in a state of inertia, what systems or actors move the wheels of oppression? How does technology become a mechanism in deepening inequality? This comparative study will examine the political implications of the proliferation of digital surveillance and data driven

algorithms in modern life in the United States and China. These two nations are key to understanding how this technology is being developed and implemented because not only are they considered innovative leaders in the sector, surveillance technology has become a normative tool in both states. In this sense, digital technologies and engagement with algorithms are already widespread, adapted by state powers, corporations, and civilians, and irrevocably entrenched in civil society. I find that the domination of hierarchical structures is consequential in the execution of digital technology, thus it is important to examine how they affect the already uneven power dynamics between police and civilian populations which are heavily policed.

The United States has had globally unprecedented rates of incarceration since the 1970s and China, more recently, has come under international scrutiny for their heavily militarized police state which scholars claim targets a vulnerable population of Uighur muslims. Despite the different political and ideological regimes, it is within the authority of punishment and policing to deliver the most extreme criminal sanctions through which the embrace of technocratic surveillance algorithms produces dangerous, yet eerily similar oppressive paradigms. The implementation of data driven algorithms into these systems known for human rights abuses, requires urgent comprehension and action. Most scholars call on Western leaders in the US and Europe to implement regulations and privacy safeguards to not only promote a more liberal democratic model for surveillance to counter the leading technology in China, but also curtail the incursion on many aspects of our social or private lives. In this breadth, I find the opportunities for resistance are indeed greater in the US than in the authoritative state of China. However, modern Neo-liberal concepts of universalism in human rights, identity, and liberty are historically rooted in “a Western-centric worldview, and its spread around the world

paradoxically led to the exploitation and exclusion of subaltern populations, be they women, LGBT people or the colonized' (Nowotny 2021). Therefore, David Brin's theories encouraging a broader public acceptance of the irreversible entrenchment of digital algorithmic technologies into this system are absolutely crucial to develop resistance mechanisms more effective than agitating for bureaucratic red tape.

Chapter 1 Theoretical Foundation for Digital Technologies and AI

Before we reckon with the transformative effects of digital technology in modern society, it is essential to examine how boundaries of society have historically been reconciled with the innovations of technology. Acknowledging the inextricable link between paradigms of technology and the supposed progress of civil society, allows for meaningful and realistic methods of resistance or integration for those being surveilled. If technological systems functionally reproduce racial hierarchical structures under capitalism, then the societal or historical contexts which produce inequalities in the system must be understood. According to Brin, the hierarchical political relationships of feudalism have been transformed by the development of a significant middle class in modern global capitalism. Surveillance "is a French word, meaning to look down at people from above;" despite emancipatory movements and the establishment of liberal democracy, elites have and will always see (2016). Policing and prisons are an invention which exist beyond criminal deterrence as an apparatus for enhancing state and capital power through a monopoly on force. The fact that punitive control continues to expand, implementing digital surveillance into its mechanisms, while crime rates have consistently decreased over the past several decades is reflective of this mode of production rather than the technical requirements of crime control. Penal policy is the most violent element "within a wider strategy of controlling the poor, in which factories, workhouses, the poor law, and of course, the labor-market, all play corresponding parts" (Garland 2014). In this socio- economic superstructure, the fact that elite institutions both bureaucratic and private have "selectively" taken up data-driven technologies to enhance this power is not extraordinary. Neither is the attempt to divest from explicit repression to invest in the supposedly neutral, quantification and

qualification of data, standardization for social measurements, and professionalization of diagnostic and corrective power. How can we contend with surveillance and data driven algorithms exacerbating oppressive or penal aspects of social life if we fail to acknowledge how the most menacing, oppressive, extreme threats of digital algorithms to the disadvantaged are already inherent to policing?

This perspective forces an engagement with power dynamics as a productive force of technological and social dynamics which draws on Michel Foucault's theories of power and mechanisms of control derived from punitive institutions. Foucault describes the rise of prisons as a demonstration of further abstraction in the power of the law and the power that law exerts, a similar discursive argument to the power of predictive algorithms that Nowtny asserts. The transformations from monarchical power under feudalism to state power under capitalism mentioned above coincided with the invention of prisons and state authority over punishment. For example, punitive institutions and measures such as "galley slavery, transportation, forced labour, the early modern houses of correction, and even twentieth-century rehabilitative regimes, have been positively shaped by the concern to use convict labour, and are presented clear as clear instances where economic interest was the leading determinant of penological innovations" (Garland 2014). Under modern state bureaucracy, people become juridical and knowable subjects with certain rights wherein capital punishment and torture become absorbed into less visible functions of the state. This model proves useful for understanding the sometimes discretionary versus centralized use of complex systems as a mechanism for social management. The material conditions of the most impoverished in society interacting and responding in symbiosis with penal institutions fulfills the managerial objective of "less eligibility:" the

conditions of punishment must be more severe than the conditions of the working class (Garland 2014). In many aspects the civil, social and institutional experiences of the poor are similar to that of prisoners because of this strategic overlap and interrelated functionality. This has substantial economic significance because prisons are often framed as a legitimate ideological and structural solution to "idleness" or unemployment which is associated with criminality. Garland synthesizes Rusche and Kirchheimer theory that "far from being an inevitable aspect of social progress, penal reform occurs only where economic exigencies are relaxed, or when 'humanitarian principles coincide… with the economic necessities of the time;" even then these reforms can and will be the first surrendered to the mercy of market crises. (2014). While an elite class of profiteers play key roles as executors and administrators in technocratic implementation, they are dependent on a small population of AI engineers to conceive and transform data sets to algorithmic praxis usually informed by these socially weighted codes. Further down the chain of production and distribution comes the exploitation of millions of blue collar laborers like warehouse workers or delivery drivers. Employment or the threat of starvation under unemployment is a form of social control that maintains Capitalist exploitation. From Foucault's theory of punishment as a mechanism through which the state marks, categorizes, and constructs subjects, one can understand discipline as something that is delivered from the top to the bottom or a function and tool for those with power. Foucault argues that "the workshop, the school, the army were subject to a whole micro-penalty of time," in the sense that they implemented hierarchical methods and standards of control which incorporated standardized schedules and subtle punishments for a range of behaviors, despite being social and communal institutions (187). These modes of management have larger implications both for behavioral performance

and state orientation as both the institutional benefits of "order" and individual incentives and rewards for adherence to codes contribute to the maintenance of these paradigms. The domination of big tech in capitalist markets is driven by gig-economy labor; a new digital sector with visceral anti-union proclivities historically reinforced by police and new surveillance capabilities driven by their market needs. Mark Coekelbergh points out that not only are personal electronic devices produced under slave-like conditions but under data-driven capitalism "as users of social media and other apps that require our data…we are doing free labor for social media companies and their clients (advertisers): we produce a commodity (data), which is sold to corporations" (2022). From its inception, digital algorithmic technology cannot be dissociated from capitalist modes of production and oppressive labor conditions. AI systems learn and adapt in a coercive, hierarchical labor market as well as within an extremely punitive penal system which utilizes carceral and punitive ideology to address social problems. Digital algorithms learn that any form of social deviance must be met with punishment rather than care which effectively reinforces class, race, and gender stratification.

Ruha Benjamin's book on Race After Technology: Abolitionist Tools for the New Jim Code posits historical roots which connect digital technology and AI development to racial domination and exploitation. The word "robot" derives from the Czech word "robota" meaning compulsory or forced labor, so she scrutinizes the relationship between the dehumanizing rhetoric used for robots and language about master and slave dynamics. Coeckelbergh's chapter "Freedom: Manipulation by AI and Robot Slavery" takes this discursive approach connecting it to the Marxist model. He links the development of AI to capitalist systems of labor, production, and hierarchies. Technology integrated into capitalism which exploits, alienates, and criminalizes

working class laborers will be a mechanism of further disaffection. Given the unequal distribution of powers and profit from modern the digital data ecosystem, this constructs a unique niche for exploitation and oppression. The state transformed many logics in social theory and modes of punishment to become increasingly bureaucratic, professionalized, and scientific. Technical approaches to management or "the belief that science is the best and only means by which society should determine its norms and values - has colluded with the interests of politically or socially powerful groups" (Nowotny 2021). Ruha Benjamin references Khalil Muhammad's study of the early 20th century "racial data revolution" wherein the violent enforcement necessary to maintain systemic oppression was replaced by "new tools of analysis, namely racial statistics and social surveys" to develop theories on society and race (2019). Human racial, gender, and class subjectivity invaded these new processing and categorization "methods and data sources" to construct "black criminality…alongside disease and intelligence, as a fundamental measure of black inferiority" (Benjamin 2019). She emphasizes this social theory assigned certain meaning to particular codes with oppressive consequences because the label of criminal "in this era, is code for Black, but also for poor, immigrant, second-class, disposable, unwanted, detritus" (2019). As social theory was legitimized through technical approaches to categorization, mathematically driven AI models we live with now were just beginning to be developed at the math department at Dartmouth college in 1956 (*Coded Bias* 2020). This small faction of white men decided to measure intelligence by the ability to play and beat opponents in games, particularly chess. These concepts of imagery, intelligence, technology, and what matters in society we consider standard and normal values of measurement "are actually ideas that come from a very small, homogenous group of people" (Meredith Broussard

Coded Bias). Data driven-algorithms are designed to cheaply evaluate a large number of people with a bulk of information; they are specialized to find solutions within a very specific set of rules limiting the sorts of variability, flexibility, and deliberation necessary to discern comprehensive solutions to human social problems. The relatively small population of wealthy people receive the benefit of personal input, recommendations, and face-to face interviews, so under the mode of production described above, AI will be integrated into the larger institutional network of performativity tasked with managing the poor (O' Neil 2016). The concept of "garbage in, garbage out" specifically criticizes how inputting low-quality or nonsensical data, of typically underrepresented or misrepresented groups into a system "will produce low-quality or nonsensical results" regardless of the sophistication and power of the system (Garvie 3). The structures of global racial capitalism rest on anti-blackness; increased accuracy or the inclusion of black faces in digital surveillance systems under capitalism "is no straightforward good, but a form of unwanted exposure" because symbolic meanings in society of acceptable and deviant people are highly distorted by state and elite motivation to legitimize authority over punishment. Although the United States' social and theoretical context of data collection and classification is not exactly the same as that in China, the technocratic state still demonstrates the power of cultural coding according to "the invisible 'center' against which everything else is compared and as the 'norm' against which everyone else is measured" (Benjamin 2019). The digital technocratic epoch we know now is marked by the integration of fairly homogenous socially dominant classes of male computer scientists and mathematicians into an already stratified elite class. Cathy O'Neil states "like gods, these mathematical models were opaque, their workings

invisible to all but the highest priests in their domain: mathematicians and computer scientists" (2016).

The advances and developments in the modern digital sector grow at a significantly greater rate than exponential growth so the legitimization of perceived impartiality in algorithms built on subjective data sets presents unprecedented and expansive potential for exacerbating already existing inequalities. Within the Western academic and professional sphere this creates problems for transparency because comprehension, and discernment regarding algorithms is further alienated from the poor and particularly black and latino communities. In China, some of their surveillance technologies are targeted specifically at the minority population of Uyghyr muslims who are confined to work camps which mostly train them in manual and vocational labor. If people are sorted by a certain model and receive a negative outcome, the algorithm has claims to objectivity and secrecy which go mostly unquestioned or cannot because of heavily guarded corporate proprietary claims. Mathematical models are also constructing an "objective" reality and truth which can be wildly divergent from personal experience and memory; without feedback, "a statistical engine can continue spinning out faulty and damaging analysis while never learning from its mistakes" (O' Neil 2016). This creates a data loop where the model is legitimized by the machines own results proliferating highly destructive tangible consequences, a type of mathematical model or algorithm O' Neil coins a "weapon of math destruction" or "WMD" (2016). All of these barriers leave people with little recursive options after being subject to surveillance or algorithmic sorting. This violates the crucial concept of positive freedom wherein humans are granted autonomy, self-governance, and the agency to decide what is best for them. AI sorting in this context manipulates people "without respecting them as rational

persons who wish to set their own goals and make their own choices" (Coekelbergh 2022). Given the purported values for freedom and individualism in the United States, and the authoritarian bureaucratic structure of China, the potential for abuse is apparent. Anxiety-ridden studies that forewarn against these technologies are not sufficient so long as "technology makes an all powerful state inevitable" (Brin 2016). Academics and activists who agitate for stricter regulation fail to recognize that historically regulations have been weaponized against the average person, not the institutions and forces that use them most. Brin states "not once in human history did elites allow themselves to be blinded...it is not possible to keep useful technologies of surveillance from those with the interest and means to acquire them" (Brin 2016). Modern digital elites operate within a hierarchy "that allows some modicum of informed refusal at the very top" while positioning the masses on the unequal status to refuse (Benjamin 2019). The solution is not to cower and hide at this proliferation but rather to adapt, as Brin points out, like we always have: he cites the panic around technologies such as the printing press and radio which ultimately served to empower us all. Another theoretical approach to reconcile this inequity is "digital humanism" which Helga Nowotny defines as "a vision that human values and perspectives ought to be the starting point for the design of algorithms and AI systems that claim to serve humanity" (2021) Hiding from this technology further incentivizes elites to better conceal its development and use.

Notwony makes a compelling argument for understanding digital theories to help people reconcile daily social life with these systems on a large scale. In her book In AI We Trust, she approaches questions about the development of the digital Anthropocene or digital temporality and explores digital understanding under capitalist modes of production and distribution. The

scholarly understanding of the Anthropocene is “a juncture characterized by the entanglement of human activities on the human timescale with other temporalities” (2021). The scale of human influence on the Earth, resources, and biodiversity has increased exponentially over a certain period of time. Historically, the roots of a digital epoch lay in the creation of nuclear power and weaponry which relied on greater computational power. Nuclear bombs tested during this time transformed geographical landscapes and the life around them, therefore, there is an irreversible link between digital expansion and the modern sustainability crisis or the digital anthropocene. A rise in technocratic power in the US and China coinciding with proliferating climate disasters today, reflects a state anxiety over how to manage and organize the future: “digital technologies bring the future into the present, while the sustainability crisis confronts us with the past and challenges us to develop new capabilities for the future” (Nowotny 2021). The current body of knowledge surrounding AI as it stands is fairly disjointed rather than interdisciplinary and takes on different approaches, assumptions, and ultimately forecasts about the future. The alternative to digital humanism, as defined above, is a theoretical positioning of automation as a tool for efficiency and now places AI algorithms central to this process by rapidly increasing statistical understanding of language and reasoning. This theory, according to Nowotny, assumes all “unresolved problems will be sorted out by an ultimate problem-solving intelligence, a kind of far-sighted, benign Leviathan fit to manage our worries and steer us through the conflicts and challenges facing humanity” (2021). This foundation would expand the power exerted by predictive algorithms and “threaten to fill the present with their apparent certainty….[if] human behavior begins to conform to these predictions” (2021). This poses two potentially grave risks: first that human imagination becomes limited from reliance on predictive algorithms such that

the structure of the future is closed and pre-determined, second that predictive algorithms govern actions so much so that human interpersonal accountability diminishes.

Digital surveillance and data driven algorithms reinforce stratification when those in power can use them to target minority groups, however they also hold potential for heightened inaccessibility of information which could be used for accountability. Academic, professional, and administrative systems with built in racial and economic hierarchy which implement technological modes of management make it much harder for the average person, who uses the technology for convenience, to become a knowledgeable purveyor. Foucault's analysis of the panoptic model serves as an increasingly relevant critique on constant visibility or observation that comes with existing in modern hierarchal society. The development of algorithmic sorting and surveillance within the police state and functions fulfills Foucault's theory of states as unavoidable subject-making powers. As Nowotny argues, "if blindly followed, the predictive power of algorithms turns into a self-fulfilling prophecy- a prediction becomes true simply because people believe in it and act accordingly" (2021). This expansion of mechanisms of control at a systemic level marks a reconfiguration of behavioral codes that is more insidious than the public could have anticipated. Foucault argues that institutions outside of the state operate through a superimposition of models which are centered around training, correction, and transformation that produces subjects. This training needs to be coupled with constant observation and assessments, creating a useful body of knowledge for the state and other institutions that seek to organize or criminalize people. When institutional power and this body of knowledge on individuals come together, it produces scientific and professional specializations. Racially stratified access to education, and even further, access to employment as

it pertains to digital technology and AI contributes to technocratic inequality. Silicon Valley itself has an overwhelmingly white male hegemony yielding narrow investment in technological innovation which focuses on a particular subset of social interests, deepening exclusion and subordination (Benjamin 2019). This is harmful because its is not simply that "design thinking wrongly claims newness, but in doing so erases the insights and agency of those who are discounted because they are not designers, capitalizing on the demand for novelty across numerous fields of action and coaxing everyone who dons the cloak of design into being seen and heard through the dominant aesthetic of innovation" (Benjamin 2019). Predictive algorithms have expanded beyond science and state functions and are now inextricably tied to the economy and the social fabric. Insomuch as they can be "harnessed by the marketing and advertis[ing] industry, instrumentalized by politicians seeking to maximize votes, and quickly adopted by the shadowy world of secret services," the ideology behind this transformative power is highly distorted as a public service rather than a tool of the state or elite class (Nowotny 2021). Therefore oppression is not an innate feature in technological development, but is more accurately a reflection of how existing power and social hierarchies under global capitalism shaped its production and implementation.

Conflict theorists following the marxist tradition cite performative punishment as the unequal distribution of discipline and justice across classes where the elite class gets lighter or even non-criminal consequences for deviance. I find this argument useful for Nowotny's invocation of performativity- the concept that "what is enacted, pronounced or performed can affect action"- when describing the power of predictive algorithms. She states that this placebo effect of predictive algorithms is simply that "an algorithm has the capability to make happen

what it predicts when human behavior follows the prediction" (2021). If penal processes like policing are and prisons are legitimized in their categorization of poor individuals as criminals through the diffusion of their mechanisms in society, predictive algorithms infused with policing data would perform this same task. Using a critical analysis of class and power dynamics outlined above, powerful actors have a financial, political, or social investment in this performative power which in turn makes the power of predictive algorithms very tangible and valuable. These developments mark what Foucault considers an expansion and legitimization of corrective mechanisms for marking individuals and a professional network in this system which serves to expand disciplinary training to capture or "save" those who are "unassimilable" (1995). Through Foucault we can understand how corrective and diagnostic powers to measure and organize people develop from state management. However, Brin points to certain eccentricities of the United States such as suspicion of authority and greater value for freedom over obedience which create opportunities for these power dynamics to yield to inversion or a more symbiotic relationship between this leviathan-like digital panopticism and its subjects. Scholars who emphasize that civil entanglement with digital systems will exacerbate inequality fail to prioritize substantive solutions to the roots of socioeconomic problems. Helga Notwony provocatively argues that "aligning the values designed into machines with human values must be preceded by aligning the values of corporations with those of digital humanism" (2021). Under Capitalism, a corporation's only social responsibility is to increase financial profit for shareholders; destruction, oppression, and exploitation are thus logical consequences of corporate construction and capitalist rules. If digital humanism. as defined by Nowtny, seeks to redirect this responsibility to "human values and perspectives" it would require complete corporate

deconstruction. Human needs directing corporate responsibility eliminates the legitimization of individual property ownership essential to Capitalism. Corporations today continue to proliferate and deny the sustainability and climate crisis which threatens all of human existence because if maximizing shareholder profit requires mass death, Capitalism will kill. How can corporations and the digital algorithmic technologies they own suddenly fulfill the values of human life if a system of individual ownership allows the discretion to kill? Brin states that "if neo-Western civilization has one great trick in its repertoire…that trick is accountability" especially when that accountability reaches the wealthy and powerful" (1998). The privacy heralded in liberal society is zealously guarded by corporations and bureaucracies which conceal algorithmic processes because of intellectual property claims to digital technologies. We value both privacy and accountability but paradoxically, if given the choice between the two, people demand privacy for themselves and accountability for everyone else (Brin 1998). This is especially poignant when it comes to Silicon Valley oligarchs who superficially support environmental regulation, healthcare expansion, greater tax scrutiny on the rich, and governmental regulation in every other sector but their own. Imprinting abolitionist praxis in accountability, restorative justice, and community care as human values in algorithmic development and implementation is antithetical to hierarchal capitalist schema, therefore; embracing digital technologies with a redistributive goal forces the reckoning with and transformation of the capitalist infrastructure which produced it. This comprehensive approach to digital democratization would recognize that agitating for transparency and accountability for the most powerful would require some concessions of privacy and transparency on our part.

Nowotny invites us to consider the implications of digital advancement in a growing climate and sustainability crisis. A gap exists between the public imagination and engagement with digitized systems undertaking daily personal tasks versus complex systems predicting impending climate catastrophe. She argues that this gap can be reconciled through "the increasingly important role played by prediction, in particular by predictive algorithms and analytics" (Nowotny 2021). As we further develop and understand our computational power, she inquires "how can this knowledge be harnessed to counteract the risks we face and strengthen the resilience of social networks"(Nowotny 2021)? The power of predictive technologies rests on human action, or inaction, and as such must be understood within the context of their production and consumption. While predictive analytics can be ignored they are consumed "in a digital package that we gladly receive, but rarely see a need to unpack" while being "produced by a system that seems impenetrable to most of us, while often jealously guarded by the large corporations that own them" (Nowotny 2021). Predictive technologies have gained popularity in an increasingly digitized world as a way of ascribing some level of knowability and human control onto a turbulent future. Nowotny cites the Covid-19 pandemic as a clear example of this technocratic and scientific approach to solutions that was soon hijacked by political motivations. We will see how the power of predictive systems served both productive and insidious functions during this time. The urgency of a global pandemic led to a rapid increase in data processing to predict and chart the course of the pandemic; this overshadowed the earlier advocacy which questioned the quality of the data that fed algorithms. State power and management can obviously expand and contract as was shown with the contraction of bureaucracy at the beginning of the Covid-19 pandemic. If an unequal distribution of power creates the opportunity

for abuse or weaponization of technology against the masses, what would redistribution look like? Resistance and civil disobedience are embedded in American jurisprudence and Hannah Arendt argues that disobedience is a requirement on moral grounds (Coeckelbergh 2022). Brin outlines inverted surveillance or the concept of "sousveillance" he defines as "looking back at elites from below" as a power balancing mechanism (Brin 2016). This approach already has a foothold in the American political imagination and has had notable legislative successes. Brin notes the passage of the Freedom of Information Act (FOIA), truth in lending laws, and laws for financial disclosures of political players. From the policing perspective, a 2013 court decision determined citizens have a right to record police. The establishment of this right "to record interactions with authority was an absolutely vital event; for what recourse has any average person, when confronted by overwhelming disparity of force, other than the truth?" (Brin 2016). He states that this law has resulted in slow changes by police because they are worried about being watched. People experience fear or perceive risk "and multiply in a factor" relative to have much control they have over the situation; a digital approach which allows for communal control would quell public anxiety over tyrannical abuse of technology. With the implementation of AI, the degrees of control get further away because not only is there a lack of control between a policeman and the subject of policing, a predictive algorithm may even take a degree of control out of the hands of the police which deepens anxiety and distrust. This anxiety stems from liberal values in democracy or equal governance. As Coeckelbergh states, "AI creates new power for the technocratic steering of society, which contrasts with democratic ideals" because it undermines the principle of self-rule (2022). Brin's approach subverts power dynamics while establishing a two-way system of surveillance that can be helped by more technology not less.

He claims that calls for worry and concern over this technology is not a very productive method of resistance or accountability against elites because it does not maximize possible beneficial outcomes. If individuals gain the power to surveil those who manage those systems or "apply those lie detectors on politicians? Focus those sociopathy alerts on corporate heads? Might that mean Big Brother...never?" (Brin 2016). However, the integration of AI technology into this civilian system of accountability would require "fair distribution of expertise and power, incentives need to be created for individuals to understand AI and its supply chain" (Coeckelbergh 2022). Brin proposes an important alternative to regulation where everyday citizens are equipped with the same technological tools as the police because people have always found ways to integrate and adapt to daunting and transformative technological developments in society. Does this alternative have the potential to mechanize liberation, or undo oppression if policing has the same function? The equalization of transparency in the current digital era has the potential to dismantle many aspects of institutional hierarchy and oppression if it can eliminate the need for its most violent enforcers. This requires redistribution of unprecedented profit and power through information to open the door to other institutions which exacerbate oppression, death, or destruction and could only possibly pay with their existence. Societal or communal consensus on what behaviors are socially harmful and worthy of communal awareness, does not require an ideology of punishment; data driven algorithms in the abolitionist model would be inextricably linked to radical technology of holistic, humanist care. This paper will place a critical lens on who owns digital surveillance technology, where they are being implemented, and the political implications of data driven algorithms for resistance movements in China and the United States. My goal is to provide a comprehensive framework for the understanding and

use of digital technologies to provide the general population with clear pressure points that can be leveraged to democratize and evenly distribute the benefits of technological innovation.

Chapter 2 China- A Paragon of Digital Dominance

Introduction

It would be difficult to comprehensively understand the United States' surveillance models and incorporation of predictive algorithms into policing without an examination of China's surveillance state. China has not only successfully confined and reinforced their physical borders, but has also managed to securitize the internet and digital experiences of their citizens. In this chapter I argue, The Chinese Communist Party (CCP) has developed the most advanced surveillance state in the world; these unprecedented leaps in technology, implemented and consolidated for digital national security, lend to the prospect of a Chinese surveillance model with AI technology tuned to perfection which they use for development projects and technological expansion abroad. As they are emerging as a global leader in AI technology, they are in a powerful position to set legal and systemic norms for its use and implementation. Despite the awareness of two polarized superpowers, investment in surveillance technology in the United States and China comes from the same ideological justification: "smart city" discourse. The smart city, as defined by Simone Tulumello, focuses on the future as a way of managing present problems and conceptualizes "urban problems as a matter of technological and technocratic solutions" rather than material solutions like healthcare or housing (2021). China has made the "smart city," using technology to develop and improve urban and social infrastructure, a key part of its national development. Their "definition of smart city [is] initially

assimilated to ‘safe city; and the development of surveillance networks for the state security authorities,” emphasizing a carceral framework (Ekman and Esperanza Picardo 2020). As of 2019 they claimed to have “a total of 500 smart city pilot projects ready or under construction” (2020). Many scholars point to China as a model for digital authoritarianism where technology is used “by authoritarian governments not only to control, but to shape, the behavior of its citizens via surveillance, repression, manipulation, censorship, and the provision of services in order to retain and expand political control” (Khalil 2020). I argue that despite different socio-political foundations for the implementation of algorithms in the US and China, the roots of digital oppression lie in uneven power structures which purport scientific or mathematical “analogies that ease the transmission of ideas while stripping them of the context in which they arise” (Nowtny 2021). Given the undeniable global influence of this polity, it is difficult to imagine a surveillance model without a foundation for algorithmic oppression through unfettered exercise of power through data and surveillance technology. We will discover the significance of specific domestic and international projects developed to further China’s technological reach.

The framework for the Chinese digital state as well as one of the greatest and daunting technological achievements has been the Great Firewall, operational since the early 2000s and controlled by The Cyberspace Administration of China or (CAC). This internet structure is a sovereign “interconnected system of laws and regulations that determines acceptable and prohibited content” (Khalil 2020). This is when the international community began to take China’s goal for dominance in the information and communication technology (IT) sector very seriously. They have an expansive surveillance network within the borders, implemented as anti-crime and anti-terrorism initiatives, which includes more than 200 million closed circuit

cameras providing data to programs like SkyNet, a police monitoring system, or Sharp Eyes which links cameras from smartphones, vehicles, and personal appliances with surveillance cameras (Khalil 2020). After fortifying their surveillance structure, China personally invested in a digital aspect of the Belt and Road Initiative (BRI), called the Digital Silk Road (DSR) which has "generated US $17 billion in loans and investments in telecom networks, mobile payment systems, and projects such as smart cities, e-government, smart education, digital health, and other big data initiatives throughout the developing world" reaching about 80 countries (Khalil 2020). These systems transcend borders and national spaces because the "body is not simply seen, but is now an entity onto which all sorts of information are attached" (Rosier 2018). Through this initiative, "Chinese companies secure legal rights to data collected via Chinese tech embedded in infrastructure projects;" they are not only recreating their framework in other countries, but creating a network for data to travel to their centralized digital core, reinforcing their role as a leader in the sector (Khalil 2020). These projects have an emphasis on China establishing an international foothold however, I argue the shift from material infrastructure investments like railroads and dams to digital surveillance technology fueled by algorithms and data growing and innovating at exponential rates, creates increasingly carceral solutions for vulnerable communities which have little recourse. Facial recognition leads in Artificial Intelligence (AI) technology with over 7,837 facial recognition firms in the state (Beraja et. al 2021). We will look at the implications of this extensive carceral organization system through China's development of their Social Credit System, their intensive digital repression in the Xinjiang region, and the state management of the Covid-19 pandemic.

China invested in and innovated surveillance technology systems to provide data for China's comprehensive and controversial Social Credit System (SCS). The SCS is both a technological database and governance regime with the goal to boost society's integrity and stability through incentives and punishments based on individual's behavior in social, political and economic spheres or interactions with the judicial system (Chen, Lin and Liu 2018). The technology and algorithmic sorting used by the SCS require an extensive amount of training data to develop accuracy; Beraja and others point to the shareability of data and suggest access to massive amounts of "government data has contributed to Chinese firms' emergence as leading innovators in facial recognition AI technology" (2018). The state is extremely data rich both because complete digital transparency has been integrated within its larger political ideology and the CCP ensures that all private companies are open or at least have backdoors for government access; the Study Strong China App, required for party members, has over 100 million users and the government monitors their "progress and activity" (Groot 2020). The authoritarian government that allows access to limitless data is not as fundamental to the sector or detrimental to the public as the normalization of one-sided operational transparency found in many countries with surveillance and algorithm systems. We will see these various methods of constant monitoring and predictive policing reach brutally repressive levels in the Xinjiang province where the Chinese population of Uyghur Muslims have been sequestered in reeducation camps to see how the technology can be sharpened as a weapon against targeted groups The reach of the SCS was consolidated in 2014 allowing for implementation of more invasive security technologies in Xinjiang around the same time. This huge system has allowed for advantages like data being used to automate contract tracing, however, the Covid-19 pandemic has allowed

China to expand its surveillance and normalize its authoritarian practices under the guise of controlling the virus. The pandemic itself created a crisis of information and even though the public demonstrated unique instances of dissatisfaction and resistance to government management and the technological ecosystem, there is no state precedent for digital transparency. I find that China's centralized authoritarian technology allowed them to censor or punish dissenters during the pandemic which was legitimized and normalized by state claims to national security and public health management. They used their digital strength to manage the virus, information, and oversee pandemic guidelines while also exporting the technology abroad.

Through a study of China's surveillance technology programs, we can examine China's role and digital goals on the international stage. Even though, as of 2020, "China makes only 16% of the chips supporting its technological development," the state is rich in data and training resources which is ultimately the key to greater algorithmic sophistication and innovation (Feldstein 2019). Steven Feldstein further argues that the People's Republic of China or (PRC) "is seeking to transform its chip-manufacturing capacity through investment and intellectual-property theft in order to dominate a core set of high- tech industries" (2019). China is aggressively investing in this technological advancement; the state's leadership frame it as the "new impetus for advancing supply-side structural reforms, a new opportunity for rejuvenating the real economy, and a new engine for building China into both a manufacturing and cyber superpower" (Feldstein 2019). Scholars in the United States frame this as a dystopia of digital authoritarianism, however; interestingly, these innovations were implemented because of agitation from the bottom up; the government commissioned digital infrastructure within social services to reconcile the public sentiment of diminishing trust, safety, and cooperation in

communal life. In many ways, China's digital infrastructure reflects the social needs of their national majority; the public does not express the same anxiety about digital oppression as Westerners, so where do the tensions arise? In China's racial structure, their digital surveillance and algorithm models reinforce the image of the majority by targeting their capabilities at minorities "trapped between regimes of invisibility and hypervisibility" (Benjamin 2019). The tremendous efforts to develop a self-sufficient domestic model of surveillance from production to execution is driven by the unprecedented amounts of data being funneled into an extremely streamlined database controlled by the state. Internationally, they market success using surveillance systems as a tool for countering terrorism and crime, expanding their reach through the BRI. One of these facial recognition programs was exported from China to Zimbabwe to track millions of their citizens. Officials and public agencies in Zimbabwe can benefit from the managerial benefits of digital surveillance, while China builds a more comprehensive database of different ethnicities. If the greatest expansion of digital systems is in the institutions of crime and immigration control, diversity in the data sets algorithms are trained on would just more accurately funnel people into these unjust social mechanisms. It would reflect a technocratic approach to neocolonial extraction in the digital age "in which the people whose faces populate the database have no rights vis-a-vis the data systems that are built around their biometric input" (Benjamin 2019). This critical perspective helps to understand both the Chinese surveillance model and the problems that arise from calls for a "western" democratic model to counter it. This popular media and scholarly perspective coming out of the US is complicated by with this account of similarities in carceral logics driven by economic markets and state commitment to racial hierarchy.

Chinese Social History and the Conception of Digital Infrastructure:

Unlike the United States, the Chinese government is a key facilitator, and unavoidable intermediary during every step of surveillance technology development and implementation. However, Chinese citizens place significantly greater trust in the centralized government than local communities or neighbors as arbiters of justice and purveyors of public good; The Social Credit System or SCS, particularly, demonstrates the state's attempt to mitigate this lack of social trust within its borders. It is considered a diversion from the traditional Chinese mantra of "governing the country in accordance with the law" towards a new regime of "rule of trust" (Chen, Lin, and Liu 2018). Rule of trust is "a governance mode that imposes arbitrary restrictions-loosely defined and broadly interpreted trust-related rules- to condition, shape, and compel the behavior of governed subjects," an effort according to the Chen, Lin, and Liu, attempts to fill an ideological void in the Chinese Communist Party (2018). As of 2019, the SCS system has not used artificial intelligence technologies, " real time data or automated decisions" nor has it "reached the stage where each individual is given a numeric 'score' as such in determining the person's social status," which has been misleadingly reported in US media (Chen, Lin, and Liu 2018). Development of the national Social Credit System, beginning in 2002, was primarily a financial resource for businesses and individuals that paved the way for the SCS today. It extended into the social sector with public complaints of "trust-breaking" and

"credit information barriers" in society that the SCS was equipped to address through integration and consolidation of information on individuals from other government agencies (2018). Eventually the State Council issued a plan in 2014 to build a social credit project to enhance society's integrity and establish credit standards beyond the financial sector.

The first step in consolidation was assigning every individual a "social credit unified code" or SC unicode: an 18-digit code from identity cards that link to personal data, including income, tax and social insurance payments, and financial registration information (2018). The purpose of this data is to identify those who break trust or violate legal rules, civil regulations, and even traffic laws: the result is a Black list of 23 million "trust -breaking" organizations or individuals as of 2020, and a Red list for "trust-keepers" (2018). Many city governments such as "Honest Shanghai" have established their "own credit websites to promote the SCS and to share data with agencies at the provincial, municipal and county levels" (2018). The distinction of what is considered trust breaking is very vague and the violations are not always criminal according to the law: spreading rumors on the internet is considered trust breaking and in the Henan Province "rejecting university admission after passing the national exam...is seen as a 'trust breaking' act" (2018). Chen, Lin and Liu's argument makes it clear that this idea of trust erodes the previous tradition of rule of law because the norms of trust are vague and broadening with no clear standards or restrictions for individual or social behavior. Red list individuals enjoy benefits like faster government services and less bureaucratic control like inspections. The mission behind Black lists is "trust breaking here, restrictions everywhere;" they are utilized by the "judicial, tax, customs, security supervision, environmental protection, safety inspection, transportation authorities," and more (2018). The most expansive is the nationalized "Defaulters

list," with 9.59 million individuals by the end of 2017, who have not complied with court judgements, which restricts "government procurement, bid tendering, administrative approvals, government support, financing credit, market access and determination of qualifications" (2018). This, in turn, affects their work and social life as this information is made public. Chinese concepts around shaming, trust, and governance through reward and punishment are rooted in many generations before digitization. We will look at specific examples of the more insidious and inescapable form these concepts have taken with the help of surveillance algorithms later on. Historically, however, there is a cultural emphasis on Confusian ideas of loyalty to the family and the state but not to strangers. Paradigms of technology were integrated within those cultural and political ideals through databases and social media platforms with hundreds of millions of users that share this vast data with the SCS. The social credit system of China has been characterized by western discourse as undemocratic by "excluding, punishing, and discrimination certain individuals or groups," but categorization and social sorting are not new in the West (Rosier 2018). On the other hand, there was an expression of shock and awe in the sensational tone of the discourse at the expansiveness of such an advanced system being implemented in such a densely populated nation. One of the major questions that has not been made public to the world or to China's own citizens is how criteria are used to organize people. Citizen's behaviors have only been given point values that culminate into an overall social score on a local level, such as Shanghai and Rongcheng in the Shandong province.

The only regulations for data collection were implemented through the Cybersecurity Law in 2017 against individuals and private businesses, not the government itself; "in fact, many laws and policies in China, keenly seek to facilitate, rather than deter, the government's control

of personal data" (2018). The effectiveness of SCS in restoring social trust does not outweigh its consequences because "the label of 'trust-breaking' generates new government-backed sanctions for behavior not originally condemned in the legal system, thus blurring the line between social, moral norms, legal norms wherein the "rule of trust" often trumps the traditional "rule of law"(2018). The SCS in its current form also "makes already disadvantaged groups more vulnerable to additional punishments, which is a departure from the principle of equality before the law" (Chen, Lin, and Liu 2018). And lastly, because the SCS is used by multiple government agencies, this compounds punishments for broad violations that go beyond what would be imposed in the case of individual violation of law. The SCS also restricts due process and a right to legally challenge sanctions. The only hope for an individual to be removed is for the court to remedy or recognize an error with no personal statement. The SCS's complex web of sanctions for an individual's violation extends to employment, transportation and even their family; they also extend beyond its borders. Government efforts to expand data collection have gone without significant public resistance possibly because the SCS had a role in reducing fraud such as "tax evasion, non-compliance with court-ordered payments, food-safety violations" and more (2018). China has also managed to control the media narrative blaming mostly private companies for privacy concerns. The SCS has flourished as a convenient governance tool under China's authoritarian state. However, it is the unregulated and rampant data collection from a structure of carceral "state control, unjustified social exclusion and discrimination" as well as "shrinking space for privacy, and the erosion of due process" that can be found in the democratic machine of the US as well as China that creates algorithmic oppression and a grim comparative future for surveillance under capitalism.

Surveillance and Algorithmic Repression: Xinjiang

Any fear or anxiety around the political implications of China's surveillance state reaches a zenith when one takes the Xinjiang region into account. However, the distinct digital repression exercised in this region cannot be dissociated from the social power and role of policing to maintaining hierarchies and expand forms of punitive control. The nationalized SCS has garnered a lot of attention but has not incorporated any standardized applications of predictive algorithms. This region serves as the intersection of all of China's technologic and predictive algorithm capabilities with an immense occupational police presence targeted at a single minority group. The implementation of AI into this system is insidious because it can "not only monitor individuals' whereabouts and online behavior," but can be developed "to map their relationships through link analysis, to discern their intentions or emotions using sentiment analysis, and to infer their past or future locations and actions for the purpose of regime maintenance;" this province can be considered an absolute model of digital authoritarianism (Khalil 2020). Not only are Uyghur Muslims subject to gruesome human rights abuses, they are well documented among an international community that is mostly inactive. The historical framework for China's counterterrorism efforts may be similar to other nation-states attempts to reinforce national security like the post 9/11 shift towards increased border security; however, examining the Xinjiang province specifically, China has an irrevocable economic presence that has not only legitimized the state's most extreme domestic surveillance model, but also the exportation of this counterterrorism method of surveillance to other countries. The United States does little to interfere with China's authoritarian repression of Uyghur Muslims or the trade of

their technological services. This is because in many ways, the United States is extremely dependent on Chinese exports and economic infrastructure, therefore; the extreme forms of digital oppression which occupy this region cannot be fully comprehended outside the market interactions of global capitalism. The Strike Hard campaign of 2014 is known as a key expansion of surveillance mechanisms in the Xinjiang region. The result is the largest population of an estimated one million incarcerated Muslims, particularly of Turkish ethnicity, in the world in China. This domestic counterterrorism strategy and goal began in the 1990s as well as Strike Hard "anti-crime operations to assure the public of the state's ability to provide security" against China's "three evil forces: separatism, terrorism, and extremism" (Byman and Saber 2019). The effects of 9/11 also reverberated worldwide with a shift in Strike Hard Campaigns towards "illegal religious activity and separatist ideas" in China (2019). As the definition of security has incorporated digital spaces, these ideological and political programs have sharpened a dangerous and often violent technological edge with the development of an extremely repressive police state in Xinjiang "that essentially monitors residents every move" (Byman and Saber 2019).

The intensive technological repression in this province is authorized and normalized through State claims to domestic security and counter terrorism measures to an "evolving and militant threat" (Soliev 2021). The East Turkestan Islamic Movement (ETIM), an independent Xinjiang independence and separatist movement, with a more radical sect called TIM, East Turkestan Education and Solidarity Association (ETESA), Uyghur led and based is Istanbul, and the World Uyghur Congress, an advocacy group based in Germany, are all muslim organizations with various terrorist classifications and ties to the Xinjiang region. However, Byman and Saber state that "much of what China considers terrorism at home...appears to involve individuals or

small groups rather than larger organizations" citing specific incidents of fatal political violence. (Byman and Saber 2019). There was a notable clash in 2009 the CCP blamed on the World Uyghur Congress: in Urumqi after two Uighurs died during a conflict between Uighur workers and Han Chinese, "over 1,000 rioted...resulting in more than 150 dead and over 1,000 injured" (2019). In 2014, at the Kunming train station, "eight Uighurs armed with knives killed 29 and injured 140" (2019). Within May of 2014 "a suicide bomber killed 39 at a market in Urumqi" and "one Uighur also armed with a knife injured six at a train station in Guanzhou" (2019). A government compound in Xinjiang was attacked in February of 2017 "when three Uighurs detonated a bomb outside" resulting in five deaths. (2019) Sweeping counterrorism legislation then passes in 2015, a standalone law, that "gives the government broad authorities and vaguely defines terrorism and extremism so as to encompass a broad range of actions that the regime fears would threaten domestic stability" (Byman and Saber 2019). The law does not allow the media to report "on counterterrorism without government approval"and requires that AI and internet companies contribute to counterterrorism efforts "including with decryption and limits foreign access" to China's (ICT) or information and communications technology (Byman and Saber 2019). It has received both domestic and international criticism for lack of judicial oversight, "allowing for individuals to be sent to education centers after prison sentences without clarifying the circumstances under which that can occur, and mobilizing members of the public against targeted groups through the creation of villager committees" (Byman and Saber 2019).

Chinese surveillance mechanisms in Xinjiang "escalated to include internment camps, forced labor, and daily indoctrination programs," and the government expanded into biometric data collection such as "DNA, fingerprints, iris scans, and even gait" (Byman and Saber 2019).

Their surveillance has heavily focused on carceral solutions to violence boasting that they have "punished over 30,000 people for illegal religious activity," actions that could be viewed as "legitimate religious observance or political action in other countries" are criminalized in the region. This looks like banning a range of arbitrary actions like wearing "clothes that supposedly advocate extremism" or even "storing large amounts of food or suddenly quitting drinking and smoking" (Byman and Saber 2019). Any action that could be perceived as a potential harm to stability can result in exorbitant fines or incarceration. The activities of XinJiang residents is monitored and assessed for threat through a mobile app called the Integrated Joint Operations Platform or (IJOP) which "collects personal information on all Xinjiang residents, not just Turkish Muslims, and links it to the individual's identification number," tracking location and other information as well. However, only "knives purchased by Uighurs have the purchasers' identification data etched onto the blades as QR codes" (Byman and Saber 2019). The IJOP app "notifies officials when an individual needs to be investigated" and even "provides officials with specific questions to ask during interrogations" (Byman and Saber 2019). Although this is most prevalent in XinJiang, it continues to be exported to other parts of China, especially regions like Tibet, with larger minority ethnic populations. Authorities are alerted when people under suspicion "venture more than 300 meters from their homes, workplaces, or other approved areas;" their connections and potential abilities to travel overseas are heavily monitored as well (Byman and Saber 2019).

The CCP secretary Chen Quangua first used the paramilitary grid system in Tibet before becoming "the mastermind behind the [Xinjiang] region's surveillance and re-education programs" (Byman and Saber 2019). The Sinicization or reeducation program is meant to

legitimize state oversight and control over “ethnic and religious affairs”. China has more than one million Uighurs and other Muslims in these camps and “another two million forced to attend daytime political indoctrination programs” (Byman and Saber 2019). These operations hail from a decades-long governmental effort to “bring economic prosperity to minority-majority regions” that might work “to quell separatist impulses, beginning with Xinjiang” (Byman and Saber 2019). The programs implemented since, have sought to manipulate the region’s demographics and erase many public aspects of traditional Muslim culture. The population of Han Chinese in the region has grown from 7% to 40% from 1949 to today (Byman and Saber 2019). The government promotes ethnic inter-marraige with monetary incentives, however, there is darker evidence that “Uighur women [are] being forced to marry Han men in exchange for freeing male relatives held in the internment camps” (Byman and Saber 2019). The CCP claims that the centers are focused on economic uplift to “turn the Uighur population into an industrial workforce to help lift them out of poverty” (Byman and Saber 2019). They have since legally formalized the camps with the goal of restricting Islam “within the confines of traditional Chinese culture...and make it more compatible with socialism” (Byman and Saber 2019). Detainees in camps are forced into a curriculum “reciting Chinese laws and Communist Party policies, learning Mandarin, singing songs about the CCP, and Xi Jinping, and renouncing religious beliefs” and face harsh interrogations or torture if they do not comply. Outside of camps they are still required to “attend weekly or daily flag-raising ceremonies, Mandarin classes, and political indoctrination meetings during which they are obligated to praise the CCP and condemn their families” (Byman and Saber 2019). The Chinese government has even banned clothing and outward affiliations with Islam “this includes banning the veil, fasting for Ramadan, and certain

beards; restricting pilgrimages to Mecca; and even issuing a list of banned names because of their association with Islam" (Byman and Saber 2019). This cultural restriction goes even further as children are banned from learning about or participating in religious activity in school or at home. The government has even demolished traditional Islamic centers and mosques in towns like Hasgar and converted them to recreational centers and restaurants. The state control over accepted categories of behavior without public insight into what information determines these categories is the key to surveillance repression.

As of July 2019 Shohrat Zakir, the governor of Xinjiang, claimed the majority of these groups had been released and " more than 90 percent of the discharged people had found decent jobs with local industries and manufacturing factories;" despite this, it is still unclear how many people remain in the labor camps (Soliev 2021). There is virtually no way for journalists to confirm these claims because their operations are concealed under state classifications. There is also still significant government control and oversight in these facilities and limited contact with family leaving questions about continued forced labor and continued human rights abuses. Sometimes contact is impossible because "most of their children have been placed in 'child welfare' institutions and boarding schools to learn the Chinese language and 'better life habits'" (Soliev 2021). The long term success of this overarching campaign is yet to be determined, however Soliev argues that "militant groups have framed the Chinese detentions as oppression" The China State Council Information Office issued a paper in March 2019 revealing "authorities in Xinjiang had arrested nearly 13,000 terrorists and broken up over 1,500 violent and terrorist gangs since 2014" as well as 2,000 confiscated explosive devices in the region (Soliev 2021). Despite these claims, "the majority of Uyghurs who have traveled to Southeast Asia in recent

years appear to be peaceful asylum seekers" fleeing China and traveling through Malaysia and Thailand in attempts to reach Turkey, the home of a large Uyghur community (Soliev 2021). Calls for greater transparency in the region particularly from the U.N. are criticized for political motivations that "maintain a double standard in how they choose to label terrorist attacks in China versus the Middle East" (Byman and Saber 2019). This is fairly true as the United States, the most powerful U.N. member, "sees the Uighurs and other Muslim communities as oppressed when it gives them any thought at all" and "prioritizes terrorism in the greater Middle East" (Byman and Saber 2019). Fear of China's economic retaliation was made clear when 22 mostly western states signed a letter on July 2019 calling on China to respect human rights, but not a single country would take credit for leading the effort; furthermore 37 states "primarily Middle Eastern and African states...submitted a letter commending China's human rights achievements and the success of its counterterrorism program" (Byman and Saber 2019). Thus, China's strategy of counterterrorism has been legitimized within the neoliberal international parameters concerning human rights, despite evidence to the contrary, because their digital sovereignty allows for complete technological discretion and their international influence discourages pushback. Both factors are crucial to the state's surveillance advancement and promotional goals.

COVID-19 Pandemic

The CCP has responded to the spread of a global pandemic by utilizing large amounts of citizens' data and activity in collaboration with The Cyberspace Administration of China (CAC) to not only control the Corona virus but to control the narrative about the government's management, considering the international blame for the crisis. Many scholars point to expansion

of an already worrisome model of digital authoritarianism wherein criticism is met with "further censorship and propaganda both within China and through external diplomatic efforts" while dissenters are arrested and detained (Khalil 2020). The spread of the Covid-19 pandemic has also led to an increase in and consolidation of digital authoritarian functions like AI "surveillance cameras, drones, facial recognition technology, big data collection and analysis, tracking apps, and QR codes linking travel history and medical data" (Ekman and Esperanza Picardo 2020). Companies developed health apps to determine risk and cameras were installed outside homes or apartment buildings to deter people from breaking quarantine while the CAC effectively suppressed any criticism of quarantine restrictions or government accountability and transparency by removing or blocking posts (Khalil 2020). Cyber sovereignty and centralized government control over internet governance and surveillance development were crucial aspects of this digital authoritarianism that reached new levels under the cover of pandemic measures. The need to control a global pandemic both "stalled an emerging public debate on personal data protection" and has provided a "proof of concept" demonstrating that surveillance technology works on an extensive scale (Khalil 2020). More interestingly, a comparative study of information governance in China's mainland versus Hong Kong during the early stages of the pandemic emphasizes the necessity and the possibility for digital transparency, especially during times of crisis when the consequences are compounded.

When the pandemic first spread in 2019, information spread on social media was dismissed as rumor; public information about controlling the outbreak in mainland China did not become available until the General Secretary of the CCP, Xi Jinping, made an announcement about guidelines on January, 20th 2020 (Ding and Lin 2021). A doctor at the Wuhan Central

Hospital in China, Ai Fen, was reprimanded by hospital authorities for “spreading rumors” and “harming stability” for trying to warn colleagues and staff about the coronavirus early on in December 2019 (Khalil 2020). Another doctor’s death, Dr Li, sparked outrage expressed through Chinese online platforms about government censorship. They were quickly removed “with the help of artificial intelligence-powered search engine tools” and “the same internet police that silenced Dr Li were efficiently dispatched to pursue netizens who had written critically about the Chinese government’s handling of the outbreak and DR Li’s treatment” (Khalil 2020). Around 897 people were detained or punished for their online activity as it relates to the Covid-19 virus. This has gone as far as companies “deleting or blocking posts from people who write about family members getting sick, ask for donations or assistance online, or give eyewitness accounts of overwhelming conditions at hospitals” (Khalil 2020). The lack of digital transparency intensified the effects of pandemic while undermining social stability.

Ding and Lin characterize how technological ecosystems operated during the pandemic: mainland China employed “information authoritarianism” while Hong Kong experienced “information anarchy” (2020). Even though both systems “failed to deliver accurate and reliable information to the public due to the spread of disinformation or misinformation,” the Hong Kong government disclosed information regularly and allowed people to share information as they pleased (Ding and Lin 2021). The greater digital freedom in Hong Kong, plagues the region with polarized media, low trust in government, and “social media misinformation;” therefore, the local government is more willing to sacrifice government power and the illusion of social stability, compared to governments in the Wuhan and Hubei province, for greater transparency and to guarantee individual rights. I argue that the proliferation or oppression of surveillance

technology in China and elsewhere is fueled by the normalization of zero state transparency. This is made especially clear through an examination of the different information management systems of mainland China and Hong Kong. Ding and Lin characterize the weeks from December 2019 to January 19th as “Phase I;” they argue local government officials in Wuhan and Hubei controlled and politicized any mention of cases to maintain social stability during the annual political meetings of local governments called“two sessions” and the Lunar New Year, a large Chinese festival (2021). They spread the false claim that “there were only a limited number of confirmed cases, no medical staff infected, and no human-to-human transmission and that the outbreak was under control” (Ding and Lin 2021). Wuhan authorities did not seriously investigate cases first reported on December 8, 2019 until December 31; afterwards they controlled release of pandemic information related to cases around government events. In Ding and Lin’s analysis of information governance in Hong Kong they frame “Phase I” from late December to January 22nd and “Phase II” as the 23rd until the end of February. Unlike the strict control of the CCP in the mainland, “the Hong Kong government has maintained an open information practice and regularly updated the situation of the outbreak outside Hong Kong in Phase I” (Ding and Lin 98). They issued public health notices when information about outbreaks in Wuhan first reached them. The Center for Health Protection or (CHP) and the Secretary for Food and Health (SFH) took many preventive measures including strengthening “inspection and quarantine at all ports of entry to Hong Kong and promoted public education on disease prevention” and continually updated information on cases detected in mainland China, Japan, Taiwan and Thailand (Ding and Lin 2021). Hong Kong’s government has the same technological capabilities and surveillance systems as the mainland; however, their management of the

pandemic lends to the prospect of a transparent, albeit less organized, surveillance state that is not at odds with individual freedoms.

After Xi's declaration of official pandemic measures on January 20th, media and news reports in the mainland surged from 28 on the day of the announcement to 241 the following day, and only increased from there. Critical state reporting tended to focus on local government officials' handling of the pandemic and "commercial media followed suit: several investigative reports criticized local officials' malfeasance and demanded political accountability" (Ding and Lin 2021). The state government effectively retained control over what was worthy of reporting and worthy of accountability. The lack of transparency in the mainland allowed for some state control and redirection of public indignation. The CCP and local governments in the mainland incorporated "Phase II" into their pandemic management: "on 21 January...the Central and local governments began to release information on a daily basis regarding COVID-19 statistics and details of confirmed cases," which was previously buried (Ding and Lin 2021). They introduced strict lockdown measures by January 29th and began using digital health codes to "facilitate reopening" (Ding and Lin 2021). Hong Kong entered their "Phase II" after two imported cases of Covid-19 were confirmed on January 23rd, the government activated the highest emergency level on the 25th. They also kept the public up to date with daily information about pandemic governmental management and the spread through press conferences or online platforms such as the CHP's online Covid-19 dashboard. Ding and Lin state that "Hong Kong has an open and free media system structurally and cherishes freedom of press as an important core value of the society" (2021). They followed the Covid virus closely, both locally and globally, interviewing scientists and experts while also highlighting or criticizing the government response. Operating

under less censorship, they could more readily challenge disinformation from the mainland and take a more critical stance towards officials. A "pro-democracy centrist" newspaper, called *Ming Pao* for example, reported on January 5th "that the Jinyintan Hospital of Wuhan disallowed medical staff to take leave in order to handle a sharply rising number of infection cases, which never appeared in Mainland media" (Ding and Lin 2021). Through information transparency, citizens were guaranteed more methods of recourse and resistance to government measures that proved effective. The importance of this in combatting the pandemic was emphasized and published by scholars and media in Hong Kong. During "Phase II" the political polarization of the public began to as there were many contentious debates around banning visitors from Mainland China from traveling to Hong Kong, shortage of personal protective equipment (PPE), particularly face masks, and quarantine and screening sites designated by the government (Ding and Lin 2021). Many locals organized and participated in protests and strikes around certain government measures; the outcry for face masks even "pushed the government to carry out a local mask production subsidy scheme" (Ding and Lin 2021). Government services in Hong Kong were driven by the public's perception while the mainland focused on guiding public perception in support of state services.

Despite instances of criticism and resistance of the mainland government from the public on IT platforms, "the strict censorship on conventional news media and institutionalized governance over social media significantly offset such empowerment" (Ding and Lin 2021). The mainland's information system was ultimately ineffective because "rumors as resistance" were used to battle against government disinformation and misinformation spread. Hong Kong's consistently open information system sparked both public debate and collective action resulting

in “information anarchy” because “the media and the public have the freedom to produce and disseminate pandemic information” (Ding and Lin 2021). The public in Hong Kong, because of digital information transparency, asserts significantly more checks and balances on their government than the people of mainland China. Therefore while surveillance technology is becoming increasingly unavoidable or repressive during catastrophe, there are also models and opportunities for resistance or accountability through transparency. China has not been alone in its use and promotion of surveillance technologies to curtail the pandemic with many democracies such as Australia, Taiwan, and India implementing Covid tracing and protection apps out of which “only 12 countries have introduced systems that meet the full five-star criteria, in that they are voluntary, have limits on how the data is used, require that data is not retained, minimize data collection, and are transparent in design and use (Khalil 2020). This framework for concealed or “black box” surveillance is not unique to China and as a result neither is the potential for algorithmic oppression.

Conclusion China’s Global Vision

President Xi Jinping has promoted the vision of a “digital panopticon” in China, which is an “all-seeing digital system of social control, patrolled by precog [future vision] algorithms that identify potential dissenters in real time” (Khalil 2020). Institutions and companies such as the National IT Development Strategy, Alibaba, Tencent, Baidu, Made in China 2025, and China Standards 2035 have helped position China to achieve that goal and “define global technological standards and to...project the CCP’s geostrategic goals” (Khalil 2020). The influence of China as a technological leader is clear given the role of the SCS has spillover effects outside the Chinese

border. Businesses hoping to establish a foothold "during the course of business registration...will receive an SC unicode and become subjects of the SCS," foreign airlines and NGO's are included within SCS databases and their behavior is categorized by trust (Chen, Lin, and Liu 2021). They also use passports and other travel documents for foreign actors to determine a social credit and even require commercial companies such as Airbnb to "proactively hand over information on foreign guests to government authorities, including their passport numbers and dates of stay" (Chen, Lin, and Liu 2021). China has pushed private companies to seek international contracts because they are "key for the national economy and continue to move up the value chain and for generating new sources of growth through their internationalism" (Ekman and Esperanza Picardo 2020). They continue to heavily invest in these technologies and have now become the world's largest supplier of surveillance technology according to The Carnegie Endowment for International Peace (Groot 2020). Companies like Huaweii, Hikvision, Duhua, and ZTE currently present themselves "as a 'leading provider of Safe City and Smart City solutions' and, by the end of the 2019, Huaweii had signed 73 'safe city agreements for surveillance products or services across 52 countries," like Serbia and the Philippines (Ekman and Esperanza Picardo 2020). The AI startup Cloudwalk Technology signed a contract with Zimbabwe's government "to provide facial-recognition technology for use by state-security services" (Feldstein 2019). This influence, however, is limited in the EU. Beyond donating technology under what they consider an "anti-epidemic" model, China also promotes their smart city systems through educational training programs and lectures for engineers, government officials, and business professionals from developed countries especially. They emphasize the security, political, and social benefits beyond the pandemic for all countries. The

Bureau of Industry and Security in the US (BIS) has banned US firms from doing business with particular Chinese tech and surveillance companies like Huaweii yet, “a number of U.S companies are contributing to the development and entrenchment of China’s surveillance program” (Byman and Saber 2019). U.S internet companies are also given the controversial choice between fulfilling “China’s wishes on surveillance and content or push for free speech that may be exploited by communities China accuses of being linked to terrorism” according to Byman and Saber (2019). Many companies have chosen the former seeing as China effectively built a network “of capitalist gold valued information of citizens, wanted by governments, accordingly to generate security and protection for individuals, or to support the power structure of authoritarian surveillance practices” (Rosier 2018). This international network of surveillance oppression fueled by limitless access to data, legitimized by state claims to classified security, and reinforced through carceral force and international power is chilling; however, more alarming is that these political foundations for algorithmic abuse are present in the United States.

Marking these notable similarities within this comparative study I argue that the United States will more likely double down on the technocratic solutions of surveillance technology for a liberal “democratic” model of surveillance use. The proliferation of China’s repressive state through these technologies has not yet been a reckoning that leads to greater transparency and regulations in capitalist democracies, but rather confirms their success as tools of social control. Much of the United States’ technological and strategic development after 9/11 is done within an orientalist structure of relative positioning. Orientalism, within the American context, is the recognition or construction of a Japanese, Korean, and Indochinese other in order to develop a deeper understanding or connection to cultural goals and ideals (Said 1978). From an academic

and political perspective it is the accepted “basic distinction between East and West as the starting point for elaborate theories, epics, novels, social, descriptions, and political accounts concerning the Orient, its people, customs, ‘mind,’ destiny, and so on” (Said 1978). I do not want to fall into the orientalist trap of othering China but rather reflect on its development as a lens into surveillance “perfection”. This country has its own extensive history of mass incarceration of minority groups as well as expansive surveillance mechanisms used against suspected communists and black freedom movements during Cold War McCarthyism through COINTELPRO. Ideals surrounding democracy or human rights have historically been undermined in the US during social upheaval to control and delegitimize the state’s political opposition. Predictive policing reproduces these historical injustices rather than improves security. Western discourse on China as a method of reflection and communication is utilized to construct and reveal a dystopian reality through political media and scholarship. It is generally very negative and highly critical, reflecting the “SCS as a thoroughly negative and worrisome development for China’s citizens” that induces “anxiety around the world” (Rosier 2018). It is often described as Orweillan or similar to dystopian stories depicted in Netflix’s *Black Mirror*. In the west, however, the proliferation of these technologies is much more silent with citizens' personal data being framed as an “economic good” volunteered by consumers. Rosier argues that “this justifies the creation of the ‘transparent citizen’ and creates a neoliberal world order” where the collection and trade of private data is not considered a human rights violation (2018). China’s investment in technological development has yielded them significant profit and economic success which the United States is heavily invested in as well. People in the US engage on the internet and sites through social media or “cookies” used by private companies to collect

information which may “contribute to production of neoliberal subjects who approach the world through the eyes of consumers rather than those of citizens entitled to rights” (Rosier 2018). Thus, the normalization of government and corporate discretion over digital transparency is just as insidious in the United States surveillance model as the authoritarian regime in China.

According to Byman and Saber, the United States and other liberal democracies “are still setting the global counterterrorism agenda” to a degree, however, “China has found opportunity to independently strengthen ties with that states face terrorism threats” (2019). They have been very successful in promoting this extensive and repressive use of technology as a counterterrorism model abroad in Pakistan, Kazakhstan, Nigeria, and other countries in sub Saharan Africa by using “its soft power to suppress criticism of its tactics” (Byman and Saber 2019). Beyond the criticism of undemocratic human rights violations in this region, “neither the United States nor other countries have shown more than token concern for China’s mass incarceration and surveillance programs” (Byman and Saber 2019). Byman and Saber argue that stems from a China’s economic dominance wherein other countries rely on China’s “economic influence as well as arms sales, surveillance assistance, and limited security cooperation to gain their support in general and for terrorism-related issues” (2019). Exports are used to strengthen China’s own surveillance capacity, for example, “Chinese firms are working with Etiopia, Ecuador, Bolivia, Brazil, Venezuela, and other states to help them monitor political opposition and journalists” (Byman and Saber 2019). Venezuela, in particular, developed the “fatherland card” database from the Chinese telecommunications company ZTE which the Chinese government can access and use to innovate its algorithms. The United States has historically exercised similar power especially when it comes to monitoring and eventually extraditing their

political opposition and restricting freedom of speech of journalists such as Edward Snowden and Julian Assange. As a member of the U.N. China has “ratified nearly all U.N conventions related to counterterrorism” and has even “advocated for U.N. members to agree on a definition of terrorism that can serve as the foundation of future counterterrorism work and for U.N. counterterrorism to address the supposed root causes of terrorism such as poverty and the desire for self determination” (Byman and Saber 2019). China playing a more active role in the shaping of the debates and measures that make up the counterterrorism approaches that claim to reflect liberal values demonstrates a legitimization and normalization of China’s position and influence on the global stage.

Chapter 3 The United States of Punishment

I was immediately drawn to the political existential crises digital technologies have forced around concepts of liberty, privacy and identity in the United States because these supposed values are structurally limited by mechanisms of punishment and policing. The United States has reached globally unprecedented rates of this technocratic, penal data-harvesting with 113 million people who have an immediate family member who has ever been to prison or jail (Sawyer and Wagner 2022). Despite extraordinary uprisings and global collective action against prisons and policing, 1 in 3 people in the US has been touched by the criminal justice system and billions of dollars continue to be funneled into the most violent and extreme institution for managing social problems. Policing mechanisms in this country obviously do not directly correlate to crime rates because penal reach has extended to more people as crime rates have constantly decreased. How does penal power expand while less people are available to convict and imprison? This network derives from the “Broken Windows” theoretical approach of nearly

40 decades ago which assumes community solidarity through informal social control capacities are threatened by fear of disorderly people, or disreputable behavior. In this social framework, major violent crimes can be prevented by positioning police as the first response to small scale disorder or non technically lawbreaking deviance. This model promoted the expansion of the informal social control capacities of policing as a solution to "urban decay" (Kelling and Wilson 1982). The majority of evidence reveals "misdemeanor policing," as it is now understood, to be criminogenic and creates the conditions where people are more likely to commit crime. Issa Kohler-Hausmann's piece on the increased criminalization of misdemeanor offenses in New York City highlights the managerial, processing, and categorization mechanisms of the criminal justice system as a part of state functions beyond managing crime. She discovers that most misdemeanor cases move through the system over a long period of time, yet eventual get dismissed without any conviction. She notes these interactions with the justice system as processes of "marking, procedural hassle, and performance" which extends far beyond the supposed goal of criminal control. She examines a crucial question: if the criminal justice system is not labeling misdemeanor offenders as criminals, how are they categorizing or managing them and why? She argues that a focus on imprisonment doesn't capture the full reach of penal institutions. Her analysis of misdemeanor policing reveals how criminal justice processes abdicates adjudicative responsibility for a more managerial intention: procedural records keeping for programs and officials to figure out what the type of person is in front of them and manage "adherence" or progress over a period of time (2013).

This perspective positions punishment, prisons, and policing, as central social phenomena "which has a set of determinants and social significance which go well beyond the technical

requirements of crime control" (Garland 2014). Evidence of this method of social management reveals a criminogenic mechanism; it departs from the adversarial model of comprehensive fact based sentencing trials which funnels discretionary power to prosecutors who can unilaterally decide whether a person is guilty, a case is worth trying, and how to leverage sentencing. Defendants have little insight into these processes and little recourse once a sanction is delivered; the time and cost required for self-advocacy to challenge these sanctions is transferred to individual. Legitimized through penal legislation, the cost of criminal law administration has been passed on onto civilians through civil assets forfeiture, victim assistance fees, parole service fees, mandatory surcharges and more. Criminologists generally have to reckon with the many processes of policing and punishment which are dissociated from crime but rather functioning in the broader domain of capitalist social hierarchy and organization. Policing and criminal institutions have the authority to attach significant identity markers to individuals deemed criminal or deviant, yet; these societal codes have had little deterrent effect on criminal activity in general, but rather mark, process, and categorize subjects situated in "a network of power-knowledge by recording facts of their actions and status to be used by officials in other areas of social life" (Kolher-Hausmann 2013). In contrast to AI implementation in China, US innovation is less informed by the social needs of the public but by the needs of the market. Notably law enforcement officers claim that they feel more pressure, from the top down, to use algorithms because of the hierarchical structure of their management. Development and innovation in the digital sector of the US is heavily driven by commercial and private actors who can exercise unilateral discretion around algorithmic processes. I argue that digital surveillance or data driven algorithmic technologies integrated into United States social life will reproduce

the oppressive paradigms of racial capitalism because the main purveyors of social goods, corporations, the state, or police, arbitrate social service versus punitive solutions to social problems along racial, gendered and class lines. Insomuch as police are a central social apparatus or extension of state corporate power, we can understand and diminish the most extreme impact of algorithmic oppression through a critical lens on the mechanisms of policing. Academics have four criticisms of predictive policing. First, copyright protections limit or eliminate transparency and there is little to nonexistent governmental oversight or communal avenues for accountability. Second, the obvious concerns that they rely on extensive data collection that could threaten individual rights to privacy. The third concern deals with confirmation bias or the "garbage in garbage out theory" in AI design, and finally, If predictive policing will target the broad range "misdemeanors and nuisance crimes" which as we found earlier have no implication on public safety but rather furthers a process of urban or "territorial stigmatization" (Tulumello 2021). The scariest consequences of algorithms are already inherent to policing: penal mechanisms create a symbiotic coding signal between the poor or disadvantaged and criminality, they can irrevocably mark individuals yielding significant social barriers, the density of bureaucracy and jurisprudence has made justice inaccessible or incomprehensible. Transparency is a crucial element of restorative justice or abolitionist movements which call for communal accountability and non-punitive approaches to punishment. Digital systems and algorithms can easily be integrated to reinforce this communal model, however, the superstructure of capitalism gives police and corporations unilateral discretionary power over digital transparency. As Benjamin poignantly states, "innocence and criminality are not objective states of being that can be detected by an algorithm but are created through interaction of institutions against the backdrop

of a deeply racialized history" (2019). This chapter will look at specific case studies of cities in the US to examine how digital surveillance systems are integrated into mechanisms of policing which already strategically expose, monitor and mark oppressed people. We will consider the political implications of this penal foundation for those who seek to develop comprehensive methods of resistance and self-determination.

Origins of Technocratic Management Ideology

Scientific and technical approaches to social management have long been legitimized by those in power as a process of modernization. In this process, it has often colluded with those in power as a legitimized weapon of control or eugenics to cull the unwanted and redefine humanity in society. The idea of policing or predicting crimes before they happen works with the same anticipatory logics that have been crucial in earlier technocratic governance, the criminal justice system, urban management policy more generally (Tulumello 2021). Digital surveillance and data driven algorithms integrated into this supposed progress constructs the "digitally recognized face" as an "entry point to everything known about the past, and geared to predict future behavior" (Nowtny 2021). This approach to digitization draws on a short term, ahistorical and mostly speculative theory of technology in the "smart city" as the determining factor for the progress of civil society towards the ideals of equality and justice. Smart cities are broadly defined as a city that functions "as a complex system of systems" wherein "a constellation of technologies-networked sensors, ubiquitous communications, big data analytics, algorithms-enabling real-time management and control of complex urban dynamics" (Tulumello 2021). Urban problems are tackled through data collection and analysis because of the perceived

rationality and objectivity of these systems. The basic underlying assumption of predictive policing is that "crime is not randomly distributed across people or places;" it rather draws on dominant criminological theories that crime derives from "environmental conditions, situational decision-making, chronic offenders, and social networks" (Brayne and Christin 2020). Predictive technologies are implemented in police work with "risk based deployment" that focuses resources on algorithmically determined hotspots and "automated data grazing to flag potential crime series...difficult for any one person to identify (Brayne and Christin 2020). Within criminal courts, they use risk assessment algorithms to "structure decision making" (Brayne and Christin 2020). They are applied to predict a defendant's probability of threat to public safety or appearance in court in the pre-trial process and utilized during proceedings for sentencing decisions. From there, they have been implemented to predict recidivism rates and influence parole decisions. Within the structure of prisons and jails themselves, algorithms "determine the security classification of incarcerated individuals" (Brayne and Christin 2020). Legal rules and procedures have extensive variability in the process of application, enrollment, and monitoring beyond formal guidelines of conviction. Kohler-Housmann argues that they are tools "managing marginal populations that construct the status of current and potential recipients and regulate their sense of entitlement and their relationship to the state and labor force" (2013). To assume that all of these mechanisms work toward conviction and punishment, mis-conceptualizes the functional role of policing within society and how algorithms would enhance that role.

Neoliberal ideology or strategy that uses the urban environment as testing locus for technocratic solutions to social problems is what Tulumello describes as "urban

entrepreneurialism" or "corporatization of urban services; dismantling of welfare programs; and over-securitization of public space" (Tulumello 2021). By means of penal mechanisms, the poor can be regulated in ways that are not just about delivering or withholding services or goods, and this social function extends even to those not actively receiving benefits. Radical perspectives invert this narrative with a critical lens on the symbiotic relationship between the material conditions of punishment poverty. Departments which have implemented technology early on, ultimately led to a notable decrease in the size of the force, increased administrative control over the public sector, and transformations in political or civil relationships to safety. In his study, Tulumello sets out to fill a gap in critical discourse of the "smart city" that lacks perspective on the expansion of surveillance technology and predictive algorithms in policing by looking specifically at the implementation of Blue CRUSH (Crime Reduction Utilizing Statistical History), a predictive policing program developed by IBM in Memphis, Tennessee starting in 2006. Within this context the implementation of Blue CRUSH citywide "can be understood as part of a broader trend towards algorithm-based policymaking" (Tulumello 2021). Blue CRUSH specifically is a GIS based predictive policing program that makes "use of real-time data from reports by police officers and intelligent CCTV with plate recognition software," the implementation of it in Memphis, was heralded as successful in reducing crimes in the city nationally and worldwide (Tulumello 2021). Police and policy makers claims that the program resulted in a "26% drop in serious property and violent crimes from 2006-2012, a 31% reduction of serious crime and 15.4% reduction of violent crime, and that the scaling down of Blue CRUSH in 2011 increased crime rates" (Tulumello 2021). The last claim was found to be false, the claims of reduction were true for some crimes; however, when placed in a longer and more

national context property crimes follow national trends that have been decreasing since the mid 1990s. In conclusion, "official crime data do not offer any empirical ground to conclude Blue CRUSH may have had any impact on crime" (Tulumello 2021). However its city-wide expansion points to "austerity" in urban policy making that is marked by a gradual shift of public resources from social programs in Memphis "towards circuits of accumulation" and securitization through a slow increase in MPD funding even when the number of officers goes down (Tulumello 2020). Given the spread of these systems in cities in the US, noted above, this proliferation can be positioned as a feature of a larger neoliberal political project to make city governance more affordable, privatize or commodify police, and cities "as a site of consumer driven accumulation" (McQuade and Shah 244). The emphasis on digitized security and consumer consumption will be the basis for how algorithms determine solutions to social problems and public services. These changes are features of what Bennet et.al determine to be a post 9/11 Neoliberal security state. Looking at the city of Chicago specifically, sweeping surveillance and record keeping by authorities is not new, police infiltrated and surveilled countless leftist organizations through the Subversive Activities Unit going back to the late nineteenth century (Bennett 2017). After 2001 these records were digitized into the system CLEAR (Citizen Law Enforcement Analysis and Reporting) which allows police to "access criminal and case histories, outstanding warrants, 911 calls, crime scenes, license plate data, suspect details, police booking photographs and geographical crime data" (Bennett 2017). Chicago's Emergency Communications Center (CECC) was merged with the Crime Prevention and Information Center (CPIC), reorganizing the Chicago Police departments around command centers "made the data -driven managerialism associated with ILP possible" (Bennett 2017).

This history gives context for the expansion of surveillance technology in Chicago and the use of high visibility cameras known as Police Observation Devices (POD). POD or intelligence-led policing (ILP) is policing that uses surveillance, intelligence, big data, geographic information systems and other technologies to monitor urban areas as a method of "preempting potential risk and minimizing future loss" (Bennett 2017). The CPD was the first force in the United States integrate facial recognition technology into cameras with an initial installment of 30, in 2003 to over 20,000 in 2014 (Bennett 2017). The technology has developed from capabilities such as zoom, 360 rotation, and night vision to include gunshot detection, smaller hybrid PODs, wireless, remote control, and facial recognition supported by the 4.5 million photos of arrested crime suspects provided by police (Bennett 2017). Integration of institutional and private sector surveillance cameras into this police network increased CPIC access to 25,000 cameras throughout Chicago (Bennett 2017). Facial recognition software however is primarily used for license plate recognition with the implementation of Red Light Cameras; whether or not this has led to a reduction of traffic related accidents is unclear. The financial incentive is more apparent with 500 million in city revenue resulting in tickets issued since 2007 (Bennett 2017). These all derive from different procedural and deployment tactics known to policing: the analysis of current crime hotspots and predictions on where crime might develop in future neighborhoods as well as identifying people at risk using social network analysis. While a 2006 poll found that 58% of people supported Chicago's video security network, many grassroots organizations in Chicago like We Charge Genocide and The Chicago Alliance Against Racist and Political Opression are agitating for change and police accountability. Issac and Lum conclude that the disproportionate effects of this policing have detrimental repercussions for urban communities

that are “disproportionate to the level of crime, [amounting] to discriminatory policy” (2016). These concerns must be taken seriously to challenge and hold policing accountable. The justification for broad surveillance is that it aids current investigations while preventing future crimes. While there is little data to support this except in locales with high crime with visible cameras, the presence of this technology in all neighborhoods regardless of crime rates is, according to Bennet et al, indicative of a fanciful concept of safety around civil activity and consumption.

Garbage In, Garbage Out

Algorithmic representation of race adds to a much larger historical image archive where visual conceptions and representations have long been the battlegrounds of racist science, literature, and popular culture for decades (Benjamin 2019). 2018 MIT lab report called “Gender Shades: Intersection Accuracy Disparities in Commercial Gender Classification” concluded that out of 1,270 people facial recognition software “worked best on white males and failed most often with the combination of female and dark-skin individuals with error rates up to 34.7%” (2018). With the ushering in of digital systems to manage civil populations, this creates new and interesting concerns for image making and representation. Clare Garvie’s study of the use of facial recognition software by the New York Police Department (NYPD) reveals unique and informal mechanisms for identifying suspects. In 2017, police were looking for a suspect of petty larceny at a CVS in New York. The store surveillance camera caught a partial photo of the suspects face which an officer noted looked like the actor Woody Harrelson; they then used

google searched high resolution images of the actor rather than the actual photo of the suspect in their face recognition algorithm to identify a match to the suspect photo. This match was sent to investigative officers who arrested the suspect. This illuminates the problem that “there are no rules when it comes to what images police can submit to face recognition algorithms to generate investigative leads...these images may be low-quality surveillance camera stills, social media photos with filters, and scanned photo album pictures" (Garvie 2019). Facial recognition systems are part science and part art where some photos must be edited, adjustments go further than simple lighting adjustments for clarity, before submitting them in algorithms for a search. The NYPD used editing techniques to replace “facial features or expressions in a probe photo with ones that more closely resemble those in mugshots-collected from other people” (Garvie 2019). They also remove facial expressions “such as the replacing of an open mouth with a closed mouth” or “graphically replacing closed eyes with a set of open eyes in a probe image,” generated from a google search for a pair of eyes” and many others (Garvie 2019). These alterations reinforce fabricated identity points where “the original photo could represent 60 percent of a suspect’s face, and yet the algorithm could return a possible match assigned a 95% confidence rating (Garvie 2019). Operating within punitive institutional power allows for discretionary and informal rules for algorithms, the consequence of which have little to do with the processes of algorithms themselves, as it would not have marked people as a suspect without specific input, but more to do with underlying policing infrastructure. At least half a dozen police departments across the country permit, if not encourage, “the use of face recognition searches on forensic sketches" (Garvie 2019). Composite sketches are inherently subjective and dependent on a victim's memory. Garvie specifically cites a case from Washington county that Amazon web

services used to demonstrate face recognition software capabilities to identify suspects from sketches showing inaccurate practices are endorsed by both the private companies who provide these systems and the police who use them. Studies done outside and within police departments find that face recognition systems are not designed to accurately match sketches to photographs, they often fail or worse misidentify, yet the practice persists. The only oversight standard currently is "many law enforcement agencies, the NYPD included, state that the results of a face recognition search are possible matches only and must not be used as positive identification" or for "investigative leads only" (Garvie 2019). Police departments claim that face recognition is a step not a final one in identifying a suspect yet people are being apprehended and arrested based on possible matches found in the software. Examples include NYPD placing a suspect in a lineup based solely on facial recognition, the results of a facial software match texted from the police department then confirmed by the victim via text as the only confirmations leading to an arrest etc (Garvie 2019). NYPD specifically made 2,878 arrests pursuant to face recognition searches in the first 5.5 years of using the technology" while a detective estimates it will be used in 8,000 cases in 2018 alone (Garvie 2019). The problem lies in the fact that defense attorneys are not disclosed on the role face recognition systems played in the arrest even though "prosecutors are required under federal law to disclose any evidence that may exonerate the excused" (Garvie 2019). Reasonable doubt of accurate identification from facial recognition software given the data/ police departments feeding them is extremely important while there is no independent oversight. The low administrative bar of "investigative leads only" might be eliminated by the FBI, who have their own face recognition system, because they believe algorithms will improve with no consideration of the data feeding them. Without regulations on data input curbing the use

of composite sketches, google or celebrity images, and edits of images, Garvie suggests a "moratorium on local, state, and federal law enforcement use of face recognition" (Garvie 2019). However, just as critical is the recognition that making algorithmic functions more accurate and inclusive for policing, only attunes and perfects the violent processes of criminalization, punishment, and imprisonment imposed on vulnerable or oppressed populations.

Garbage Consequences

In order to effectively resist, we must first look closely at the consequences of the "garbage in garbage out" theory in daily life. Issac and Lum attempt to answer questions about coded bias within predictive policing algorithms by looking at policing processes and data in Oakland, California. The proliferation of data driven programs has raised concerns for activists and citizens regarding transparency, privacy, bias, reasonable suspicion, and how data is used. This unease is supported by criminological scholarship going back to the nineteenth century that suggests "police officers-whether implicitly or explicitly- consider race and ethnicity in their determination of which persons to detain and search and which neighborhoods to patrol" (Issac and Lum 2016). As a result, police records are not an accurate measure of crime but rather "some complex interaction between criminality, policing strategy, and community police relations" and these are the processes and meaningful codes which become embedded in machine learning (Issac and Lum 2016). They look at two algorithms specifically: that of Microsoft's automated chatbot and Google flu trends to demonstrate how unrepresentative data is the problem facing algorithm usage, not the algorithms themselves. In the case of the Microsoft chatbot Tay, outside users intentionally flooded the bot with unrepresentative data while the Google flu trends predictive failure came from Google's own system. In both cases the algorithmic process of

machine learning behaved correctly but failed to meet the goals of their creation. Issac and Lum further argue that “even the best machine learning algorithms trained on police data will reproduce the patterns and unknown biases in police data” (Issac and Lum. 2016). Particularly because of their assertion that this data is reflective of police activity; thus, predictive policing “is aptly named: it is predicting future policing, not future crime...selection bias meets confirmation bias” (Issac and Lum 2016). To support this thesis, they compare national data on drug use, to police methods and records of arrests in Oakland. Because police databases rely on crime and drug use that is reported and potentially criminalized, there is no local data to compare with police data. They use the 2011 data from the National Survey on Drug Use and Health to create a synthetic population of the residents of Oakland and estimate the number of drug users based on the national data. Based on their empirical data and graphic representations “it is clear that police databases and public-health derived estimates tell a dramatically different stories about the pattern of drug use in Oakland” with police presence concentrated in low income and non-white neighborhoods which experience “200 times more drug-related arrests” (Issac and Lum 2016). The use of drugs in Oakland as a whole is pretty evenly distributed (Issac and Lum 2016). They then apply the predictive policing algorithm of Predpol, because it claims to be race and gender blind by only taking in three data points: past time, place and type of crime, to Oakland police data set to analyze the accuracy of predictive policing algorithms using police records. They find that the algorithmic model does not have the capacity to correct biases in the police data and can only reinforce them; the algorithm failed to flag criminally underrepresented white and wealthy neighborhoods where drug crimes did occur. They then test whether this creates a feedback loop wherein police deployment in crime hotspots determined by the

algorithm reinforces bias that drug crimes are not committed outside zones where police deployed. They find that targeted policing according to the PredPol algorithm increases "the number of crimes observed by 20%" which feeds into the crime predictive forecast of the future (Issac and Lum 2016). Here we see the foundations of policing as a criminalizing process; the integration of algorithms into this mechanism creates a digital layer of criminal or deviant labeling. Further abstracting police activity from supposed criminal activity on the ground. Digital systems are interestingly legitimized as a way to tailor accurate police response in communities; paradoxically this legitimization means the police are more likely to respond to algorithmic signals of criminality (fed by their own practices) than to actual crime rates. Next, we will examine an internal study of police and courts which focuses on police sentiments and approaches to using these new digital systems.

Reception of Algorithms in the Criminal Justice System

This ethnographic study seeks to examine the reception of algorithms both by police departments who have implemented them and the courts which examine them. Predictive policing is defined above, but criminal courts also "use multiple predictive instruments, called 'risk-assessment tools,' to assess the risk of recidivism or failure to appear in court among defendants'" (Brayne and Christin 2020). These researchers sought to remedy pitfalls in scholarship on criminal justice algorithms particularly the treatment of the criminal justice system as a monolith and failing to "analyze the contexts of reception," assuming algorithms are implemented uncritically (Brayne and Christin 2020). To address this they analyze two ethnographic studies: one in a police department and the other in a criminal court. There are three similarities between them, first all actors used big data as a predictive measure, second both

presented algorithms as "more rational and objective than 'gut feelings' or discretionary judgements," and third they find similar strategies in resistance like "foot dragging," ignoring the tools in daily work" and "data obfuscation" (Brayne and Christin 2020). The biggest difference is that judges and court officials could use the technology at their discretion while police officers felt managerial pressure from the top down to integrate algorithms into their tasks. The study was done at the Los Angeles Police Department between 2013 and 2015 and the criminal court fieldwork was done in 2015 in an anonymous urban county, with a notably much smaller population, in a southern state. They found two main predictive policing models within the police department. Person based models gave individuals on the street a points value and a numerical rank based on points assigned for violent criminal history, gang affiliation, probation or police contact (Brayne and Christin 2020). The Crime Intelligence Detail then made lists of chronic offenders with "name, date of birth, CII number (rap sheet number), driver's license number, physical descriptors, physical oddities (such as tattoos or scars), arrest history, CalGang designation, parole and probation status, warrants, vehicles, recent stops, and police contacts-for individuals with the highest number of points" (Brayne and Christin 2020). Beginning in 2012 they also implemented a "place-based predictive software program, PredPol, to identify areas where crime was most likely to occur in the future;"police are recommended to spend at least 10% of their patrol in these hotspots (Brayne and Christin 6). This algorithm claims to be race and gender blind by only relying on three inputs: past time, place and type of crime. Both the criminal courts and LAPD demonstrated a fear of "function creep" wherein the data and surveillance they use to do their jobs is then implemented on a managerial basis to surveil their productivity or decisions. This is not far from reality because so many aspects of their job are

measured and quantified (Brayne and Christin 2020). More interestingly, it reveals that those with power, have the same anxieties over privacy and transparency that we do. Another fear was that algorithms devalued experience and past knowledge in the professional sphere of officers or prosecutors so "technocratic oversight associated with big data analytics represents a threat of deskilling" (Brayne and Christin 2020). Officers resisted by foot dragging and visiting hotspots at their discretion while judges did not always use the risk assessments at their disposal. Data obfuscation was more common, for example, a series of antenna malfunctions that turned out to be the result of officers removing them to interfere with voice recognition systems "and prevent management from hearing what they are saying in the field" (Brayne and Christin 2020). Criminal courts on the other hand sometimes refused to share their data with other departments all of which contributes to more hidden discretionary power among these actors. Ultimately, like other eras of technological transformation, police and criminal institutions are wary and reluctant to integrate digital systems into their everyday work. This perspective is crucial because it demonstrates clear points of conflict which can undermine the power of police, and the oppressive capabilities of algorithms in their hands.

Conclusion

Western democracies like the United States failing to regulate surveillance capitalism while expanding predictive policing programs have led to citizens becoming "habituated to restrictions of liberties and increased monitoring- particularly if they are managed via inconspicuous or convenient digital technology" (Khalil 2020). Consumers are already reliant on data-mining platforms and the state has the technological capacity to expand surveillance mechanisms and abuse algorithms. While surveillance is largely accepted in Chinese regions,

there have been diverse forms of collective action and individual resistance to surveillance and facial recognition technologies; protestors have worn masks and tried interfering with camera feeds. These have been partially effective, but the greatest collective public power comes from information transparency as seen in Hong Kong. Whether or not citizens in the United States will be able to reverse the use of these surveillance systems to expose the state to public accountability rather than commercial or social convenience is yet to be determined. With the impending threat of mass migration due to the Climate crisis, the US will continue to expand surveillance mechanisms in order to better manage and organize the population. However, the Covid-19 pandemic, as well as the Black Lives Matter movement related to police killings, which were key instances of social upheaval and crisis, increased public digital engagement and awareness of technological tools as methods for organizing and resisting the state on a national level. A 2013 court decision determined citizens have a right to record police and the establishment of this right "to record interactions with authority was an absolutely vital event; for what recourse has any average person, when confronted by overwhelming disparity of force, other than the truth?" (Brin 2000). This was a crucial moment where the state felt the un-batting eye of public surveillance and people were encouraged to use their phones to record instances of state violence. Through this weaponization of personal technology against the state, people were able to counter official state narratives and legitimizations for violence with undeniable digital truth. While a free and equal flow of information has been a tumultuous system in Hong Kong, with less public trust in government and rampant misinformation; I believe that even with regulation under US capitalism, algorithmic technology will still be irrevocably oppressive. The

best recourse for citizens is agitating for information transparency and surveillance democracy wherein the watched can also be the watchers.

There is a gap between the intended effects of digital surveillance and the actual material effects of predictive technology. As algorithms are continually being presented as a reliable technocratic vehicle to usher institutions and civil society into the future, they are informed by the strength and enduring role of discretion, power, and dominant culture which they reveal through their impact on socio-economic paradigms. The foundation for abuse of digital algorithms lies in the integration into capitalist hierarchy which promotes discretionary power over its AI functions and processes. Algorithms create an existential crisis of autonomy, identity, and privacy across all aspects of society, and it is nearly impossible to imagine curbing digital expansion. This sort of logic is also relevant in describing the expansion of punitive power of prisons; algorithms in this system extend carceral and detention power beyond the structure of prisons through wearable tech and surveillance mechanisms. Nowtny states that “there will always be situations full of ambiguity for which data extrapolated from the past is insufficient or far too standardized to provide answers relevant to the diversity that pervades local contexts” and as such we must value a critical eye and human wisdom or ethos to determine what could be done differently. This societal difference, according to Benjamin, is “also an artifact of marketing, mission statements, and willingness of designers to own up to their impact” (2019). Through constant agitation and critical reflection, people can transform digital technologies with an emancipatory or decarceral function. For example a converter app, called Appolition, was created by a black trans tech developer from California to redirect people’s change from purchases to black bail funds (2019). This is one of many possible digital solutions which

subverts power dynamics while establishing a two-way system of surveillance that can be helped by more technology not less.This is just the beginning of divesting from penal mechanisms because they have been expanded and legitimized in other institutions of social management in which digital systems play only a small part. Police are structurally positioned to deliver violence and oppression, abolitionists who seek to replace violence with models of communal care, must reckon with the ways in which the prison has been reborn in our schools, our workplaces, our home, and within ourselves such that the integration of digital algorithms is shaped by the demand and power to transform institutions.

Bibliography

Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." California Law Review 105, no. 3 (2017): 735–76. http://www.jstor.org/stable/44630759.

Arnett, Chaz "Race, Surveillance, Resistance" Publisher: Ohio State University. Moritz College of Law Citation: Ohio State Law Journal, vol. 81, no. 6, 1103-1142, (2020). Type: Article ISSN: 0048-1572 URI: http://hdl.handle.net/1811/92358

Barrett, Lindsey, "Ban Facial Recognition Technologies for Children—And for Everyone Else" (July 24, 2020). Boston University Journal of Science and Technology Law. Volume 26.2, Available at SSRN: https://ssrn.com/abstract=3660118

Benjamin, Ruha. *Race after Technology: Abolitionist Tools for the New Jim Code*. Cambridge, UK: Polity, 2019.

Bennett, Larryy, et al., editors. *Neoliberal Chicago*. University of Illinois Press, 2017, https://doi.org/10.5406/j.ctt1s47658.

Beraja, Martin, Y. Yang, David, and Yuchtman, Noam "Data-intensive Innovation and the State: Evidence from AI Firms in China" Working Paper No. 27723 August 2020, Revised August 2021

Brayne, Sarah. "Big Data Surveillance: The Case of Policing." *American Sociological Review*, vol. 82, no. 5, [American Sociological Association, Sage Publications, Inc.], 2017, pp. 977–1008, http://www.jstor.org/stable/26426413.

Brayne, Sarah and Angèle Christin. "Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts." *Social Problems* (2020): n. Pag.

Brin, David. *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?* Reading, Mass: Perseus Books, 2000.

Brin, David. "Will There Be Privacy in the Transparent Society?" The Journal of the Hannah Arendt Center for Politics and Humanities at Bard College, vol. 4, 2016, pp. 73–84.

Byman, Daniel L, and Israa Saber. “Is China Prepared for Global Terrorism? Xinjiang and Beyond.” Brookings Institute, September 2019. https://www.brookings.edu/wp-content/uploads/2019/09/FP_20190930_china_counterterrorism_byman_saber-1.pdf.

Chen, Yu-Jie and Lin, Ching-Fu and Liu, Han-Wei, “Rule of Trust: The Power and Perils of China's Social Credit Megaproject”. Columbia Journal of Asian Law, Vol. 32, No. 1, 2018, pp. 1-36, (April 30, 2018). Available at SSRN: https://ssrn.com/abstract=3294776

Coded Bias. United States: 7th Empire Media, 2020.

Cox, Spencer. “Bursting the Bubble: The Emerging Tech Worker Movement at Amazon.” In The Cost of Free Shipping: Amazon in the Global Economy, edited by Jake Alimahomed-Wilson and Ellen Reese, 225–37. Pluto Press, 2020. https://doi.org/10.2307/j.ctv16zjhcj.21.

Crumpler, Lewis and A.William, James. “Questions about Facial Recognition” Center for Strategic and International Studies (CSIS), 2021, http://www.jstor.org/stable/resrep28766.

Ding, Chunyan, and Fen Lin. “Information Authoritarianism vs. Information Anarchy: A Comparison of Information Ecosystems in Mainland China and Hong Kong during the Early

Stage of the COVID-19 Pandemic." China Review 21, no. 1 (2021): 91–106. https://www.jstor.org/stable/27005556.

Ekman, Alice, and Cristina de Esperanza Picardo. "TOWARDS URBAN DECOUPLING?: China's Smart City Ambitions at the Time of Covid-19." European Union Institute for Security Studies (EUISS), 2020. http://www.jstor.org/stable/resrep25030.

Feldstein, Steven. "Types of AI Surveillance." *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, 2019, pp. 16–21, http://www.jstor.org/stable/resrep20995.8.

Ferguson, Andrew Guthrie. "Big Data and Predictive Reasonable Suspicionn." *University of Pennsylvania Law Review*, vol. 163, no. 2, The University of Pennsylvania Law Review, 2015, pp. 327–410, http://www.jstor.org/stable/24247848.
Copy

Ferguson, Andrew Guthrie. "Illuminating Black Data Policing" Publisher: Ohio State University. Moritz College of Law Citation: Ohio State Journal of Criminal Law, vol. 15, no. 2 (2018), 503-525.Type: ArticleISSN:1546-7619 (print)URI:http://hdl.handle.net/1811/85816

Ferguson, Andrew Guthrie. "The Legal Risks of Big Data Policing" (2018). Articles in Law Reviews & Other Academic Journals. 1390.

https://digitalcommons.wcl.american.edu/facsch_lawrev/1390

Foucault, Michel, 1926-1984. *Discipline and Punish: the Birth of the Prison*. New York: Pantheon Books, 1977.

Garland, David. "The Political Economy of Punishment." Essay. In *Punishment and Modern Society a Study in Social Theory*, 83–110. University of Chicago Press, 2014.

Groot, Gerry. "SCHEMES, DREAMS, AND NIGHTMARES: CHINA'S PARADOX(ES) OF TRUST." In China Dreams, edited by Jane Golley, Linda Jaivin, Ben Hillman, and Sharon Strange, 198–212. ANU Press, 2020. http://www.jstor.org/stable/j.ctv12sdxmk.22.

Iapaolo, Fabio and Simone, Tulumello. "Policing the future, disrupting urban policy today. Predictive policing, smart city, and urban policy in Memphis (TN)." *Urban Geography* (2021): 1-22.

Khalil, Lydia. "Digital Authoritarianism, China and C0VID." Lowy Institute for International Policy, 2020. http://www.jstor.org/stable/resrep27665.

Kelling, George L, and James Q Wilson. "Broken Windows: The Police and Neighborhood Safety ." The Atlantic. Atlantic Media Company, July 20, 2020. https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/.

Kohler-Hausmann, Issa. “Misdemeanor Justice: Control without Conviction.” American Journal of Sociology 119, no. 2 (2013): 351–93. https://doi.org/10.1086/674743.

Prof. Issa Kohler-Hausmann on Misdemeanor Arrests. YouTube, 2018. https://www.youtube.com/watch?v=F6hcAtUFVD0.

Lum, Kristian and Isaac, William. “To predict and serve?”. Significance, 13: 14-19, 2016, https://doi.org/10.1111/j.1740-9713.2016.00960.x

Nowotny, Helga. *In Ai We Trust Power, Illusion and Control of Predictive Algorithms*. Cambridge, UK: Polity Press, 2021.

O'Neil, Cathy. Weapons of Math Destruction. Harlow, England: Penguin Books, 2016.

Perkowitz, Sidney. “The Bias in the Machine: Facial Recognition Technology and Racial Disparities.” *MIT Case Studies in Social and Ethical Responsibilities of Computing*, no. Winter 2021 (February). https://doi.org/10.21428/2c646de5.62272586.

Rosier, Maj-Britt. “The invisible surveillance: An Analysis on the Western Newspaper Discourse on the Advanced Technological Surveillance State, on the Case of China's Social Credit System” (2018).

Said, Edward W. *Orientalism*. New York: Pantheon Books, 1978. Print

Sawyer, Wendy, and Wagner, Peter. “Mass Incarceration: The Whole Pie 2022 | Prison Policy Initiative.” Prison Policy Initiative, March 14, 2022. https://www.prisonpolicy.org/factsheets/pie2022_allimages.pdf.

Soliev, Nodirbek. “CHINA: Xinjiang Province, Counter Terrorist Trends and Analyses” vol. 12, no. 1, International Centre for Political Violence and Terrorism Research, pp. 77–81, 2021 https://www.jstor.org/stable/26865754.

Weinstein, Maya “School Surveillance: The Students' Rights Implications of Artificial Intelligence as K-12 School” Security, 98 N.C. L. REV. 438 (2020). https://scholarship.law.unc.edu/nclr/vol98/iss2/12

Welch, Liam. “Grave New World: Mass Surveillance and Labour Rights.” Socialist Lawyer, no. 83 (2019): 36–41. https://doi.org/10.13169/socialistlawyer.83.0036.

Copy

Završnik, Aleš. “Algorithmic Justice: Algorithms and Big Data in Criminal Justice Settings.” *European Journal of Criminology*, vol. 18, no. 5, pp. 623–642, Sept. 2021, doi:10.1177/1477370819876762.

Završnik, Aleš. “Criminal justice, artificial intelligence systems, and human rights.” *ERA Forum*20, 567–583 (2020). https://doi.org/10.1007/s12027-020-00602-0