Surveillance & Society

Abstracting Injustice

Vincent Huynh-Watkins et Bryce Clayton Newell

Volume 22, numéro 4, 2024

Open Issue

URI : https://id.erudit.org/iderudit/1115670ar
DOI : https://doi.org/10.24908/ss.v22i4.16686

Aller au sommaire du numéro

Éditeur(s)

Surveillance Studies Network

ISSN

1477-7487 (numérique)

Découvrir la revue

Citer cet article

Huynh-Watkins, V. & Newell, B. (2024). Abstracting Injustice. *Surveillance & Society*, *22*(4), 364–380. https://doi.org/10.24908/ss.v22i4.16686

Résumé de l'article

In this paper, we explore how the neorepublican concepts of domination and antipower can contribute to the surveillance studies literature and a more democratic and participatory approach to technology development and deployment within the criminal justice system. We frame the neorepublican approach as an alternative to the predominant liberal paradigm, arguing that normative surveillance studies scholarship should emphasize the dominating potential of surveillance practices rather than merely trying to limit actual interference in peoples' lives. To illustrate, we focus on the use of surveillance technologies that capture images of individuals within the US criminal justice system for recognition and/or identification. Facial or other biometric recognition technologies (FRTs) are increasingly built on artificial intelligence and machine learning algorithms ("AI"). Often seen as a faster, more accurate, and less labor-intensive alternatives to human cognition, AI-powered biometric and facial recognition and other image capture technologies have become widely used within public law enforcement agencies around the world. The deployment of these technologies within the US criminal justice system has produced significant forms of injustice, including faulty identification and the subsequent arrest, detention, and incarceration of innocent individuals. These forms of data injustice are often opaque, hidden behind secretive law enforcement practices or commercial secrecy agreements. We draw from neorepublican conceptions of domination and antipower to frame this legal and technological opacity as an abstraction of injustice. We argue that handing important criminal justice decision-making over to code and algorithms designed, owned, and maintained by private interests exacerbates the potential for the public deployment of unjust systems that subject individuals and communities to unwarranted, arbitrary, and uncontrolled state power. Such government interference represents clear forms of data injustice and domination.

Surveillance & Society

Article | Abstracting Injustice

Vincent Huynh-Watkins

Independent Researcher, USA
vince.huynh1@icloud.com

Bryce Clayton Newell

University of Oregon, USA
bcnewell@uoregon.edu

Abstract

In this paper, we explore how the neorepublican concepts of domination and antipower can contribute to the surveillance studies literature and a more democratic and participatory approach to technology development and deployment within the criminal justice system. We frame the neorepublican approach as an alternative to the predominant liberal paradigm, arguing that normative surveillance studies scholarship should emphasize the dominating potential of surveillance practices rather than merely trying to limit actual interference in peoples' lives. To illustrate, we focus on the use of surveillance technologies that capture images of individuals within the US criminal justice system for recognition and/or identification. Facial or other biometric recognition technologies (FRTs) are increasingly built on artificial intelligence and machine learning algorithms ("AI"). Often seen as a faster, more accurate, and less labor-intensive alternatives to human cognition, AI-powered biometric and facial recognition and other image capture technologies have become widely used within public law enforcement agencies around the world. The deployment of these technologies within the US criminal justice system has produced significant forms of injustice, including faulty identification and the subsequent arrest, detention, and incarceration of innocent individuals. These forms of data injustice are often opaque, hidden behind secretive law enforcement practices or commercial secrecy agreements. We draw from neorepublican conceptions of domination and antipower to frame this legal and technological opacity as an abstraction of injustice. We argue that handing important criminal justice decision-making over to code and algorithms designed, owned, and maintained by private interests exacerbates the potential for the public deployment of unjust systems that subject individuals and communities to unwarranted, arbitrary, and uncontrolled state power. Such government interference represents clear forms of data injustice and domination.

Introduction

The "surveillance-industrial complex" (Hayes 2012), or what others refer to in various forms as "platform capitalism" (Srnicek 2017) or "surveillance capitalism" (Zuboff 2015, 2019), is central to many contemporary social control, policing, and criminal justice activities (Gates 2019). Surveillance is often addressed through liberal, neoliberal, and/or capitalist framings (Gane 2012; Murakami Wood 2013; Murakami Wood and Ball 2013), and critical surveillance scholars frequently rely on liberal rights-based theories to critique the effects of surveillance on people and society (e.g., Murakami Wood and Webster 2009; Richards 2013). However, concepts and theories based in civic- or neo-republican political philosophy also have the potential to inform our understandings of when, why, and how we might think about responding to and resisting the harms of such surveillance.

Republican ideas of freedom date back to the Roman republic, predating the classical liberal, or neoliberal, conception (Pettit 2019). Neorepublicanism refers to current attempts to apply classical republican ideas to contemporary contexts (Lovett and Pettit 2009: 12). In this paper, we explore how the neorepublican concepts of *domination* and *antipower* can add richness to the surveillance studies literature and help us understand and respond to police surveillance in ways not available within the predominant neo-liberal

Huynh-Watkins, Vincent, and Bryce Clayton Newell. 2024. Abstracting Injustice. *Surveillance & Society* 22 (4): 364-380.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

paradigm. The neorepublican approach also supports the aim of fostering more democratic and participatory approaches to developing and deploying surveillance technologies within the criminal justice system. While advocating for a neorepublican approach, we also highlight critical questions emerging in the data justice literature about the use of data and data intensive technologies by the state and show how these correspond to neorepublican concerns.

Methodologically, this paper is conceptual and normative. We draw from existing literature and media reports to develop our arguments rather than original empirical findings. From political philosophy, we draw from scholarship that extends neorepublican conceptions of liberty and domination to issues of privacy and surveillance and situate that scholarship within neorepublican theories of crime and criminal justice (e.g., Dagger, 2009; Gargarella 2009; Martí 2009; Pettit and Braithwaite 1993). We argue that *abstracting injustice*, that is, handing important decision-making procedures of the criminal justice system over to code and algorithms designed, owned, and maintained by private interests, creates real potential for the public deployment of unjust systems that subject individuals and communities to unwarranted, arbitrary, and uncontrolled state power and government interference. This development represents a clear form of data *in*justice that lines up with neorepublican conceptions of domination. We use the adoption and use of biometric and facial recognition technologies within the US criminal justice system as a lens through which to frame our larger discussion and arguments. Although our intervention here is primarily focused on US-based examples, we acknowledge these issues are confronting societies around the globe.

Linking concerns from the data justice and surveillance studies literature to these neorepublican conceptions of domination provides a useful, critical lens for evaluating the risks inherent in the use of artificial intelligence and machine learning algorithms ("AI") with image capture and recognition capabilities, including biometric recognition technologies. Using such privately developed black-boxed technologies (Pasquale 2015) within criminal justice contexts shifts responsibility for the underlying design of the state's coercive police powers to private interests and limits the ability of the state, and human beings subject to its coercive power, to interrogate their application. These outcomes enable uncontrolled or arbitrary interference by private companies and public police within policed communities. In addition, rather than only being concerned with the occurrence of actual injustices, or negative interference with a person's liberty, the neorepublican approach shows how domination rears its head and is problematic even prior to or absent any actual interference or specific incident of injustice.

In the following sections, we provide a broad overview of the neorepublican concepts of domination and antipower and then link these concepts to concerns echoed in the data justice and critical data studies literatures. Next, we outline the notion of *abstracting injustice* by discussing how AI and facial recognition technologies have resulted in multiple injustices involving the arrest of innocent people based on faulty biometric matches. Finally, we conclude by arguing that the use of such technologies in criminal justice contexts affords the state the ability to interfere in the lives of its citizens in arbitrary and uncontrolled ways that implicate the neorepublican notion of domination and raise serious concerns about data *in*justice.

Domination and Antipower

The neorepublican perspective offers an alternative to current, failing approaches to protecting privacy and other civil liberties based in liberal and neoliberal ideologies (Roberts 2023). Republicanism has been offered as an alternative political theory to liberalism. Although there is some variation in the broader republican project, the civic or neo-republican position outlined by Philip Pettit (1996) and several others equates freedom, or liberty, with *non-domination* (see also Roberts 2023) as opposed to liberal concepts of negative or positive liberty. Neorepublican political philosophy is directed at addressing "the evil of subjection to another's will" and is particularly concerned with subjection within "important areas of personal choice" (Pettit 2012: 1). In this sense, the state can play an important and instrumental role in preserving individual and collective liberty. Building on the work of Philip Pettit (e.g., Pettit 1996, 1997,

2003, 2008, 2012, 2014, 2019; Lovett and Pettit 2009; see also Besson and Martí 2009; Blunt 2015; Roberts 2023), a growing body of literature has applied these concepts to issues of privacy and surveillance.

Neorepublican conceptions of *domination* and *antipower* emerging in Philip Pettit's writings are useful to developing republican perspectives on surveillance. Building on Pettit, Capasso (2022: 182; citing Pettit 2003) has framed neorepublican liberty as "freedom of agents, not of options." Pettit (2012: 50) explains that domination exists whenever one individual or group "will be dominated in a certain choice by another agent or agency…to the extent that [the other agent] has a power of interfering in the choice that is not itself controlled by" the individual (Capasso 2022: 182). Pettit (2012: 50) argues that the power to interfere exists whenever one agent "has the unvitiated and uninvaded capacity to interfere or not to interfere" with the other person or group having no power or influence over the use of such power.

That domination can exist absent actual interference is a core feature of the neorepublican position. However, non-arbitrary (Pettit 1997), controlled (Pettit 2012), or non-alien (Pettit 2008: 16) interference is not necessarily domination (Capasso 2022: 182). Domination exists when interference is subject only to the exercised will "or discretion of the interferer; [or] interference that is uncontrolled by the person on the receiving end" (Pettit 2012: 58; Skinner 2008). As Pettit (2012: 58) has argued, "the active, intentional restriction of your choice by any other agent or agency will be invasive only to the extent that it reflects a will that you do not control."

Even when a person can make choices absent actual interference, under neorepublican theory, their domination persists insofar as another has the power or ability to interfere arbitrarily with these choices. This is the case when another agent can enact arbitrary, uncontrolled, or alien interference, thus violating a person's ability to fully self-govern without the risk or fear of such interference. This position is often illustrated using the "paradigmatic neo-republican example" (Capasso 2022: 182) of the slave and benevolent master. The benevolent master or slaveholder *never* interferes with the slave's life or choices. Liberal theories of negative liberty that define freedom as the absence of actual interference cannot explain why the slave whose master has never *actually interfered* in the slave's life might be considered just as free as her master. This is confounding to the republican, because the mere fact that the master *could* interfere with the slave's life and choices suggests that the slave is subject to domination through arbitrary, uncontrolled, or alien whims, regardless of any actual interference. This conception of domination as the antithesis of liberty has roots in ancient Rome, where concern about "the evil of being subject to a master, or *dominus*—suffering *dominatio*—…was contrasted with the good of *libertas*, or 'liberty'" (Pettit 2012: 2; italics in the original).

"Antipower" is defined as the power to resist the possibility of arbitrary or uncontrolled interference by others (Pettit 1996, 2012: 58; see also Newell 2021), or the power to "command noninterference" (Blunt 2015: 589). While not necessarily synonymous with freedom or non-domination, resistance to domination should take on characteristics of antipower through rights or activities that promote the ability of the public to resist interference from the coercive workings of the state or other entities. For example, rights to access government information, including rights to see inside the black box or enforce algorithmic transparency audits, exemplify antipower, even if they are only instrumentally valuable to contesting, challenging, or discontinuing the use of an algorithm that gives rise to domination through a loss of privacy that might expose an individual to further domination (see Roberts 2023: 39). In other words, merely being able to look into the black box and see its parts is not enough.

When people have or obtain some power to "command noninterference" (Pettit 1996: 589), they enjoy a greater measure of freedom or non-domination. Relatedly, Cohen's (2012, 2013) concept of "semantic discontinuity"—or "gaps and inconsistencies within systems of meaning" (Cohen 2012: 224)—identifies how "gaps in enforcement and in systems of surveillance and control" (Balkin 2012: 81; see also Newell 2021) can facilitate antipower. Thus, privacy, data protection, and other methods of regulating, resisting, or

avoiding surveillance are instrumental to achieving the "central ideal of modern republican theory—freedom as non-domination" (Roberts 2015a: 321). Therefore, if, "the value of privacy…lies in its capacity to shield individuals from the threat of domination" (Roberts 2015a: 321), resisting the unregulated deployment of algorithmic surveillance tools in the criminal justice system is one way to promote antipower and reduce unwanted domination.

An increasingly robust body of neorepublican scholarship is emerging in the fields of surveillance studies and privacy. For example, Hoye and Monaghan (2018) argue that neorepublican ideas can accommodate post-Foucauldian analyses to critique surveillance based on the concept of freedom as non-domination. Multiple authors have framed critiques of police use of body-worn cameras (Newell 2021; Ritsema van Eck and Houwing 2021), mass state surveillance programs (Newell 2014b, 2014c) and proposed forms of "just state surveillance" designed to prevent domination (Smith 2020) using neorepublican theories. Roberts (2023) provides the most robust argument for framing privacy in neorepublican terms (see also Roberts 2015a, 2015b, 2018), while van der Sloot (2018), Schnably (1991), and Newell (2018) also address privacy and data protection, and several other authors raise neorepublican critiques examining AI ethics (Maas 2022), digital profiling (Gräf 2017), and digital forms of manipulation and nudging (Capasso 2022).

Additionally, a growing body of critical literature focusing on data justice can be effectively harnessed in the pursuit of neorepublican critiques of surveillance. Data justice is primarily concerned with "the implications that data-driven processes at the core of surveillance capitalism have for the pursuit of substantive social and economic justice claims" (Dencik, Hintz, and Cable 2016: 9). The focus on "fairness in the way people are made visible, represented and treated as a result of their production of digital data" (Taylor 2017: 1) encompasses the "just use of digital data" (Taylor 2017: 2), "just use of data technologies" (Taylor 2017: 7), and "just data governance" (Taylor et al. 2020: 12). According to Duarte (2020: 199), data justice "presupposes a reasonable state of information equity, where factual evidence and knowledge are thoughtfully integrated into decision-making." Hoffmann (2019: 900) also argues that "bias and fairness are central themes in the emerging domain of data justice. Indeed, data justice focuses on focuses on "problems of data and discrimination" and is a counterpoint to "systems that, if left unchecked, would happily sort and segregate and optimize without regard to histories of, for example, racial or gendered discrimination" (Hoffmann 2019: 901, 900).

Importantly, as Taylor (2017: 2, citing Eubanks 2014; Masiero 2016; O'Neil 2016) recognizes, "the impacts of big data are very different depending on one's socio-economic position…[and] the greatest burden of dataveillance (surveillance using digital methods) has always been borne by the poor." These are concerns echoed in the surveillance literature, such as in scholarship building on Gandy's (1993) concept of the "Panoptic Sort," Lyon's (2003) work on "social sorting," Bigo's (2008, 2011) illustration of the "Ban-opticon," and Browne's (2015) work on racially motivated surveillance. There are ample opportunities to integrate neorepublican concerns about domination into these growing literatures, including through amplifying and advocating for the inclusion of a diverse range of voices in the development of technology and criminal justice policy.

The US Justice System

Both criminal law and criminal justice are often "forged and designed in the light of the liberal values of negative liberty and basic equality" (Martí 2009: 123). Liberal theories of criminal justice often focus on issues of punishment (Braithwaite and Pettit 1990: 1), and include retribution, deterrence, rehabilitation, or incapacitation that manifest in drastically different outcomes. For instance, under retributive justice, the offender and the threat they pose is removed from society (Meyer 1968). Deterrence theory posits that criminal law and associated sanctions operate as forms of behavioral regulation. That is, when legal punishments are "certain, severe, and swift," the individual and others will be rationally deterred from committing equivalent criminal acts (Stafford and Deibert 2007: 1065). In the same vein, regulatory theories

of surveillance are often used intentionally to "effect a desired change" in human behavior (Duke 2019: 504) and as a form of social control (Brown and Veinot 2021; Newell 2023), although surveillance can do more than simply deter undesirable behavior (Cohen 2015: 94). Theories of rehabilitation frame criminal punishment as having a "therapeutic function," with treatment "designed to effect changes in the behavior of the convicted person in the interests of his own happiness, health, and satisfactions and in the interest of social defense" (Allen 1959: 226). Theorists who question whether these theories work may consider incapacitation the most plausible justification for incarceration.

The high rate of incarceration in the US provides particularly compelling reasons to be concerned about the potential for the state's use of surveillance technologies as a form of domination in the criminal justice system. The purpose of the criminal justice system in the US is noted as reducing "crime of all sorts and to erase those social conditions associated with crime and delinquency-poverty, unemployment, inferior education, and discrimination" (Conaboy, Smith, and Snyder 1973). However, the justice system in the US carries a higher rate of incarceration than that of any other nation (Widra and Herring 2021). Young black men are incarcerated at seven times the rate of young white men (Browne 2015: 13), yet crime levels overall are no better than other similarly wealthy and stable nations (see, e.g., Grinshteyn and Hemenway 2016). Thompson (2019) argues the size of the current American criminal justice system is historically unprecedented and extremely racialized, with African Americans, Latinos, and Indigenous peoples being disproportionately represented in US jails and prisons. From the abolition of slavery to the war on drugs (see Small 2001), the systems of policing and incarceration that make up a significant part of American criminal justice have always sought to create conditions in which social mobility for black and brown people is limited.

Braithwaite and Pettit (1990: 2) argue that a broader theory of criminal justice should not focus on "harmful conduct in terms of crime and punishment" but on more productive, and less punitive, alternatives. Criminology has rationalized broad criminalization, and its attendant intrusions into the liberty of criminalized individuals, based largely on the theory of retributivism (Braithwaite and Pettit 1990: 5; Martí 2009: 125). Against the backdrop of punitiveness within the US criminal justice system, the integration of facial recognition technologies and data-driven biometric surveillance, or other image-capture-and-identification/recognition technologies, which rely on historical data and preexisting structures built by the very institutions that have subjugated entire populations, may well perpetuate these preexisting problems and result in continuing civil rights violations.

The consequentialist republican theory defended by Braithwaite and Pettit (1990) suggests that police choices about which cases to prioritize given their limited resources should be guided by whether the potential for domination inherent in surveillance is, on balance, less serious than the gain in dominion from the crime itself (Dagger 2009: 153). Rather than "the traditional police ethos [of] do[ing] whatever is necessary and lawful to bring the most serious offenders to book" (Braithwaite and Pettit 1990: 106), the consequentialist theory suggests that law enforcement should consider the seriousness of any intrusion in terms of the potential for domination that an investigation might generate. This, as the authors argue, is a vision for policing "which is responsive to dominion overall, rather than simply to crime control and public order" (Braithwaite and Pettit 1990: 107). As Gargarella (2009: 171) argues, this is a "deliberative approach to criminal justice" that is also a call for less criminal justice intervention overall (Braithwaite and Pettit 1990: 87; Martí 2009: 126).

The Application of AI Within Criminal Justice Contexts

Brayne (2021: 3) notes there has been a broad "shift toward the use of big data and machine-learned decisions throughout the [US] criminal justice system." Legal institutions from police agencies to courts are increasingly turning to commercially developed surveillance technologies to assist their work. Whether by documenting information and evidence or functioning as mechanical decision-making tools to complement

or replace human analysis (Saulnier and Sivasubramaniam 2021), AI technologies have become enmeshed in many systems of surveillance (e.g., Brayne 2021; Fan 2019; Ferguson 2017), as is commonplace in many other aspects of contemporary life (Crawford 2021; Levy 2023). AI is often seen as a faster, more accurate, and less labor-intensive alternative to human cognition.

AI technologies comprise "systems that display intelligent behaviour by analysing their environment and taking actions—with some degree of autonomy—to achieve specific goals" (European Commission 2018: 237). In policing, AI refers to the "use of technologies that apply algorithms to large sets of data to either assist human police work or replace it" (Joh 2018: 1139). Algorithms have been used by police agencies to determine whether individuals are more or less likely to become "a victim or perpetrator of gun violence" (Ferguson 2017: 37), to determine which parts of a city are more likely to experience violent crime (Brayne 2021: 86–87; Ferguson 2017: 62–64), to identify "suspicious patterns" of human behavior (Ferguson 2017: 87), to detect and identify people and vehicles as they move through space (Ferguson 2017: 93–95; Newell 2014a), and for a variety of other data-driven forms of investigative analysis (Ferguson 2017: 116–121; Guariglia 2022; Monahan 2018). This has led to a situation where "data collection, data mining, and data analysis shape both police investigation and police practice" (Ferguson 2017: 129).

These potential applications of AI in criminal justice may seem sensible and could provide fairer outcomes and increased public safety. For instance, AI-based facial recognition can help investigators and prosecutors solve previously unsolvable cases. However, these technologies can, will, and do pose significant barriers to the pursuit of a truly fair and open justice system in a functioning democratic society, often because they can compromise due process and reliability (Hillman 2019; Kaminsky and Urban 2021; Villasenor and Foggo 2020). They also raise important ethical questions of accountability and how the technologies are used to determine criminal justice outcomes. As "the emergence of biometric surveillance systems has been long described as a means for mass identification and social control" (Ramiro and Cruz 2023: 4–5, citing Lyon 2008; Pugliesi 2010; van der Ploeg 2005), these technologies offer a useful lens for examining such forms of neorepublican domination.

As generative technologies, AI "data technologies both reflect and construct justice and injustice" (Taylor et al. 2020: 14). This raises a host of legal and ethical questions about what individuals, communities, and broader society are or ought to be willing to sacrifice for overall "safety." Questions of *data justice* require an understanding "the social impacts of [what is done with] digital data" that accounts for how "(big) data systems can discriminate, discipline and control" (Taylor et al. 2020: 2, 8). "Just data governance" (Taylor et al. 2020: 12) has the goal of ensuring that people are treated fairly in the way governments and others acquire and make decisions based on data (Taylor 2017; Ziosi et al. 2024). Framed in this way, "data injustice lies in an uneven matrix of injustices" (Akbari 2019: 424). Classification or "social sorting" (Lyon 2003) is a tool of informational power that exemplifies domination, especially when its effects are arbitrary, uncontrolled, or alien (Pettit 1996, 2008, 2012). A growing number of scholars have argued that increasing automation and the consequent distancing of public decision-makers from the calculus involved in making those decisions can threaten social inclusion and social participation (Barocas and Selbst 2016; Ziosi et al. 2024) while exacerbating pre-existing biases and social inequalities (O'Neil 2016; Ziosi et al. 2024). As Ziosi et al. (2024: 1192) argue, "automation can also undermine accountability" of public institutions, such as the police and the courts.

Injustice in the use of facial recognition technologies in criminal justice is already evident. For example, in many known instances, facial recognition has incorrectly identified people, typically black men, as suspects in criminal investigations, leading to wrongful arrests (Hill 2020; Johnson 2022a; Williams 2020). Of course, human officers also misidentify people and make arrests on that basis. However, the use of facial recognition and other identification and recognition technologies could exacerbate and expand these existing problems. As is the case with other surveillance technologies, such as cell-site simulators (Nakashima 2015), uses of facial recognition or algorithmic identification technologies are not always disclosed to criminal

defendants or their attorneys (Johnson 2022b). Nor are their biases as obvious as those of a uniformed police officer. Combined with the "black box" nature of proprietary algorithmic systems used by criminal justice agencies, the secrecy inherent in algorithmic or "black data" policing (Ferguson 2017: 137) poses substantial problems for democratic governance and raises the specter of domination. One important scholarly response to these concerns has been focused on encoding forms of procedural due process into AI systems (e.g., Citron 2008; Citron and Pasquale 2014) or developing an individual right to contest AI-based decisions (Kaminski and Urban 2021).

Proponents claim that AI can function as "experts" by overcoming human error (Rigano 2019: 3), which can "increase the speed and quality of statutory interpretation performed by judges, attorneys, prosecutors, administrative staff, and other professionals" (Rigano 2019: 7–8); "predict potential victims of violent crime based on associations and behavior" (Rigano 2019: 8); and produce other law enforcement outcomes, including those that rely on facial recognition and DNA analysis (Rigano 2019: 5, 8). This framing positions AI as "a public safety resource" (Rigano 2019: 2), which implicates the privacy-versus-safety conundrum by failing to address many or all of the potential negative consequences of deploying these technologies. Opponents argue that AI systems can introduce substantial biases into procedures and decisions with life-altering effects (e.g., Leslie 2020), which questions whether they stand on solid enough moral ground to merit use in criminal justice in the first place. Although biometric identification techniques have been hailed as potentially post-racial technologies, Browne (2015: 108–109) argues the "observation, calibration, and application" of facial recognition technologies in real world settings reveals the racializing nature of these technologies. Crawford (2021) argues mythologies about *intelligence* have been used to "justify relations of domination" for centuries (4–5) and refers to the deployment of AI as "a form of exercising power" (18) in the enactment of "politics by other means" (20).

Facial Recognition Technologies and Policing

In a growing number of cases, primarily black men have been misidentified by facial recognition software as suspects for crimes and subsequently arrested (Brodkin 2023; Leslie 2020; Perkowitz 2021; Simerman 2023). For instance, in November 2022, Randall Reid was pulled over, arrested, and spent a week in jail in Georgia based on a warrant issued in Louisiana after facial recognition technologies linked his face to that of the suspect, even though Reid did not match the suspect's height or weight and, unlike the suspect, had a mole on his face (Brodkin 2023; Simerman 2023). In January 2020, Robert Williams was arrested in front of his family outside of his home in Farmington Hills, Michigan, after a facial recognition algorithm misidentified him as the perpetrator of a theft from a local store (Williams 2020). He was held in a detention center for thirty hours and only released when police later realized the algorithm had incorrectly identified him (Williams 2020). Another black man, Michael Oliver, was arrested and held in detention for two and a half days in July 2019 after facial recognition software incorrectly identified him as a match with another person wanted on suspicion of committing larceny despite non-matching tattoos, skin tone, and facial shape (O'Neill 2020). In 2019, Nijeer Parks "walked into the Woodbridge [New Jersey] Police Department to clear his name" after learning police had been looking for him at his home (General and Sarlin 2021). He was arrested based on a facial match with a fake ID left at a crime scene and spent eleven days in jail pending charges for crimes he did not commit (General and Sarlin 2021).

These examples of "false positives" provide tangible evidence of how police use of facial recognition technologies can cause harm and injustice, especially when their outputs are not understood or considered critically by the public employees who use them. However, these technologies do not function autonomously. In addition to the fallibility of AI models for biometric and other forms of image recognition and identification, some law enforcement officials have what Leslie (2020.: 26) calls "gateway attitudes" that are not actively working to eliminate and counteract sources of bias in their work. In detailing the events of his arrest, Williams (2020) questions why these technologies are used when it is known that facial recognition algorithms misidentify black and Asian people at up to one hundred times worse rates than white

people (see also Grother, Ngan, and Hanaoka 2019: 2–3). Leslie (2020: 27) classifies these examples as "part of a systemic pattern of derelict behavior rooted in the apathetic tolerance of discriminatory crime."

This pattern is more than just evidence of a harmful gateway attitude. It can also be seen as the criminal justice system working in the US in the way that it *was* designed to work, where the criminal justice system developed in response to white, settler-colonial interests in subjugating and controlling black and non-white populations, first through slavery and then by enforcing segregation (Brucato 2014: 31; Browne 2015). While the individual actions of investigators and detectives are potentially apathetic to bias and discrimination internally and within AI systems, these outcomes are precisely in line with the historical operation of the criminal justice system. The specific danger with using AI algorithms and models to affect these outcomes is that there is currently no mechanism of accountability built into this system. Seeking recourse for wrongdoing is already difficult enough. However, this becomes impossible once decisions are abstracted away to code running on a computer. Additionally, as Linder (2019: 81–81) argues:

> Platform policing…represents a problematic merger of big-data techniques with practices of targeted suspicion in which form, function, and access are primarily controlled by a corporate platform…. [This] raises crucial epistemological and political questions about relations of power. It is not, I would argue, that the simulation risks losing contact with the real…but rather the inverse: that life will start to conform to the desires and strictures of the simulation" (80–81).

In other words, the use of these systems clearly has the potential to dominate those subject to the technology's gaze while diminishing their ability to exert antipower and subjecting them to the potential for arbitrary, uncontrolled, or alien interference. In quoting Andrew Ferguson, Crawford (2021: 197) states: "We are moving to a state where prosecutors and police are going to say, 'the algorithm told me to do it, so I did, I had no idea what I was doing.'" This perspective reinforces the idea that AI use in criminal justice is just a new method of abstracting real-world justice-related harms away from responsible individuals to legitimize the algorithmic validation of undue harm, violence, and control over specific populations. If this is true, then we must question whether and how we can justify the continued deployment of these technologies. Perhaps, as Hartzog and Selinger argue, "facial recognition technology is so dangerous for society, particularly vulnerable and marginalized people, that the only appropriate governance response is to ban it" (Selinger 2022; see also Selinger and Hartzog 2020: 54). This has also been the stated position of the European Data Protection Board & European Data Protection Supervisor (2021) in relation to the use of facial recognition technologies in publicly accessible spaces, as well as several European civil society groups (Ramiro and Cruz 2023: 5). Some municipalities in the US have also banned police use of facial recognition technologies (e.g., Becker 2020; Metz 2020; van Sant and Gonzales 2019).

Platform Policing and Public-Private Partnerships

Government agencies often turn to private companies that supply software and other information and communications technologies or privately manage what would otherwise be public infrastructure or data (Brayne 2021: 5; Heydari 2022; van Brakel 2021: 229). This has resulted in what several scholars have referred to as "platform policing" (Gates 2019; Linder 2019; Wilson 2019; Wood 2019), which involves "techno-organizational domestic security configurations…[in which] private enterprises enter into legal supply-and-maintenance agreements with police agencies" (Wilson 2019: 69), or "the implementation of cloud-based platforms, built and run by private companies, that provide mass surveillance-driven simulations for a range of police operations, including predictive policing, targeted surveillance, and tactical and strategic governance" (Linder 2019: 76).

States have used data to govern their citizens for some time, but the increasing reliance "on private vendors and platforms to collect, store, share, and analyze data about its citizenry" by public agencies is more recent (Brayne 2021: 5). The development of smart cities, projects that often "frame for-profit firms as central

actors in creating efficient and innovative public services and infrastructure" (Voorwinden 2021: 439), and examples of "techno-solutionism" (Morozov 2013; Ramiro and Cruz 2023: 8), are evidence of a "neoliberal turn in statecraft" (Brayne 2021: 5). Taylor (2017: 3) argues that this neoliberal turn is central to contemporary public governance, positioning the private sector as a major player in "what we perceive as public-sector functions (counting, categorising and serving our needs as citizens)."

Brayne (2021: 5) argues that "privatization has brought the logic of risk—actuarial calculations using proprietary algorithms—to bear in ways that increasingly structure life chances…[a] shift [that] lowers the state's accountability, in part, by pointing to the supposedly neutral data wielded by private enterprise." After all, "the number of public-sector data scientists equipped to analyse big data is tiny in comparison to the number of bureaucrats interested in what big data can tell them, with the consequence that the datafication of government has been, and will always be, executed primarily by the private sector" (Taylor 2017: 3). This represents an evolution in Ericson and Haggerty's (1997) theory of police serving as knowledge or data brokers to other institutions, including private companies, in their pursuit of managing risk.

Against this risk-based framing, Gräf (2017) shows how digital profiling falls subject to neorepublican critique because it leads to domination by the state by virtue of how these algorithmic tools identify, classify, and inform state action directed at individuals, often in opaque ways driven by public-private partnerships. These public-private partnerships allow "police agencies…to 'offload the complexity' of deploying technology to private technology corporations" (Wilson 2019: 73). However, in doing so, the systems and platforms mediating the criminal justice system sometimes become more opaque and less subject to public oversight and accountability. This lack of transparency raises the specter of domination and diminishes democratic oversight while reflecting "the misalignment of public and private values, the shift from public law logic to market logics, and the insufficient range of application of public norms" (Voorwinden 2021: 451). Within the criminal justice system, algorithmic tools designed to predict recidivism risk or to calculate potential sentences for convicted criminals (Angwin and Larson 2016; Bennett Moses and Chan 2018; Symons and Alvarado 2022: 10–14) reflect this problem.

Although "purchasing equipment and technology from private corporations is not new for law enforcement agencies, the offsetting of accountability structures through evidence management is novel" (Wood 2017: 42) and represents a condition inherent in the "'grey-zones' of public-private surveillance" (Ramiro and Cruz 2023: 2). As Brayne (2021: 5) argues, "Private vendors can hide behind trade secrecy and nondisclosure agreements, ultimately circumventing typical public-sector transparency requirements and lowering the accountability of the police by making it harder for scholars to study, regulators to regulate, and activists to mobilize for or against specific practices."

Similar concerns about "limited transparency and accountability from private companies that provide the technology" have been raised in other contexts (e.g., Gräf 2017) and jurisdictions, such as Brazil (Ramiro and Cruz 2023: 2). Sometimes US federal law enforcement agencies also impose secrecy obligations on local agencies when they adopt surveillance technologies (see, e.g., Glenza and Woolf 2015; Lee and Moraff 2021). Against this backdrop, ownership and control of the data collected and generated by these platforms has become an important question (Joh 2016; Linder 2019). Platforms, such as Axon's cloud-based platform for police body-worn camera footage, function as intermediaries between the police and the public (Gates 2019: 67). However, "without strong presumptions in favor of sharing the data with the public, the reform, accountability, and legitimacy potential of body worn cameras will go unfulfilled" (Joh 2016). Indeed, "public private partnerships challenge traditional mechanisms of democratic accountability [and] public participation in policy-making processes" (Ramiro and Cruz 2023: 3, citing Grossi and Pianezzi 2017).

Resisting Domination and Data Injustice

The foregoing discussion shows how the use of facial and image recognition technologies in criminal justice contexts affords the state the power to interfere in the lives of its citizens in arbitrary and uncontrolled ways, ultimately giving rise to serious concerns about data *in*justice and domination. The public deployment of privately operated and administered technologies only exacerbates problems of public transparency and accountability. Indeed, the algorithmic opacity and outsourcing of public police powers to private companies brought to bear by the privatization and platformization of public police work stands in direct conflict with the concerns of antipower and resistance to state surveillance. If we aim for "just data governance" (Taylor et al. 2020: 12) and fairness in the use of these tools, we must do more than let the market dictate these outcomes. We need to develop and enforce transparency and auditability rules, as well as the enforcement of privacy, anti-discrimination, and data protection laws, which provide substantive accountability for both private and public actors.

Considering the evidence that AI extends or exacerbates long-standing issues of racial discrimination in the US criminal justice system, it is obvious that data justice requires us grapple with the importance of understanding "the ideological basis of data-driven processes…[and] to scrutinise the interests and power relations at play in 'datafied' societies that enfranchise some and disenfranchise others" (Dencik, Hintz, and Cable 2016: 9). Although the "concern that technological advances can have unsavory or unjust discriminatory consequences is a persistent theme in the history of computation and data processing" (Hoffmann 2019: 901), the use of AI in criminal justice settings deserves additional attention due to how the police powers of the state can have such significant consequences for individual lives.

There are at least two types of power at play in this context and that raise concerns from a neorepublican perspective. Decision-making power exists where "an individual or organisational actor A has power over B to the extent that A can get B to do something that they would not otherwise do" (Leslie et al. 2022: 28). Leslie et al. (2022: 28) argue that this form of power "is easily seen…in the way that government agencies collect and use data to build predictive risk models about citizens and data subjects or to allocate the provision of social services." Normalizing or "disciplinary power" (Foucault 1977) is evident "in the way that the ensemble of dominant knowledge structures, scientifically authoritative institutions, administrative techniques, and regulatory decisions work in tandem to maintain and 'make normal' the status quo of power relations" (Leslie et al. 2022: 29).

Leslie et al. (2022: 29) argue that when data science and AI technologies are used as "techniques of knowledge production," human subjects "are treated merely as objects of prediction or classification and…become sitting targets of disciplinary control and scientific management." Additionally, even a decision regarding whether to adopt a particular information technology can be seen as an exercise in dominating power itself and ought to be subject to effective popular control.

When AI algorithms are built on pre-existing data that suffer from bias, such as those inherent in the racist histories of policing and other criminal justice outcomes in the US (Nellis 2016), it becomes immediately apparent that using these data is problematic. It is also not clear that using synthetic data informed by pre-existing data avoids these problems. Hillman (2019: 37) refers to this problem as "garbage in, garbage out." Even with certain interventions, such as reverse engineering (see, e.g., Farid 2018), it can be difficult to know how a machine learning model has learned, or what attributes of the data weigh the heaviest in the model's predictions. As it stands, there is astoundingly little in the way of protections against these kinds of harms. The lack of recourse and opacity built into these systems (Pasquale 2015) makes the potential for dominance in the form of arbitrary or uncontrolled interference quite clear. In the case of facial recognition, innocent people can be harmed, sometimes in heavily traumatic and damaging ways. Left to develop without intervention, it seems likely that the use of AI in criminal justice will continue to unfold along the same lines upon which it has begun, by creating and exacerbating pre-existing racial and other disparities.

Morally and legally, it remains obvious that facial recognition models are largely obfuscated from any critical public view, including that of the defendant in a criminal case. This creates situations rife with the opportunity for bias to be introduced without the ability for those affected to know or have any recourse; that is, to enact antipower. This information imbalance creates the very conditions necessary for domination to occur. Privately engineered decisions with substantial real-world impacts should not be obscured in such a way, particularly when potentially racialized and class-based decisions are being made by actors who have no verified or verifiable credibility.

Conclusion

Our discussion indicates that we should call the use of facial and image recognition technologies and biometric surveillance in policing and criminal justice an *abstraction of injustice* that leads to potential arbitrary interference into the lives of individuals by governments and private entities working in conjunction. These tools are mechanisms for avoiding responsibility for poor or unjust criminal justice decision-making, giving public agencies cover to point at flaws in facial recognition models by shifting blame when something goes wrong. They also reinforce the existing focus in criminal justice policy and practice on retribution, deterrence, and incapacitation rather than attending to the more "deliberative approach" (Gargarella 2009: 171) embodied in the neorepublican call for less criminal justice intervention overall (Braithwaite and Pettit 1990: 87; Martí 2009: 126). As noted earlier, the neorepublican vision for policing is one that is "responsive to dominion overall, rather than simply to crime control and public order" (Braithwaite and Pettit 1990: 107).

Those endorsing the use of AI in criminal justice justify this state of affairs from the view that data-driven decisions are better, more informed, less biased, and automated. However, increasing automation distances public decision-makers from the calculus involved in making decisions while threatening to undermine social inclusion (Barocas and Selbst 2016; Ziosi et al. 2024) and exacerbating pre-existing biases and social inequalities (O'Neil 2016; Ziosi et al. 2024). If data justice can be advanced by "collective empowerment through democratic action" (Leslie et al. 2022: 30), neorepublican commitments to the ideal of non-domination, and the importance of institutionalizing resistance to domination, or antipower, can provide a theoretically rich foundation for motivating and pursuing these ends.

Examining the affordances that AI technologies bring to criminal justice contexts highlights how their use promotes the continued consolidation of informational power within corporations and public criminal justice agencies. This development results in the potential for domination and the loss of individual and collective freedom. As such, the use of AI technology in the criminal justice system requires great caution. We already see complex criminal justice tasks can be further complicated by incorporating AI. Rather than simplifying the process, introducing models into these systems erects opaque walls of technical knowledge. Facial recognition and other biometric technologies seemingly simplify the job of an investigator yet may lead to a lack of critical human analysis, as seen in the cases of Michael Oliver, Robert Williams, and others. When considered against existing profit motives, vague notions of "AI Ethics" or "AI for Good" are potentially non-enforceable.

When considering Pettit's (1996: 589) notion of "antipower" as increasing the ability of individuals or a community to "command noninterference" and resist domination, any regulatory response must produce substantive and procedural rights, as well as mechanisms and obligations of transparency and accountability. It should account for the deficits of procedural due process inherent in the current system of automating criminal justice (Citron 2008; Citron and Pasquale 2014; Kaminski and Urban 2021) as well as for the substantive forms of domination that often result in unjustifiable intrusion and loss of liberty. Importantly, "non-domination requires access to and the institution of effective antipowers, not courtesy and promises" (Hoye and Monaghan 2018: 359). Rights to access information, including rights to see inside black boxes or to enforce algorithmic transparency, as well as privacy, data protection, and similar methods of regulating,

resisting, and avoiding surveillance, exemplify antipower and are instrumental to achieving the "central ideal of modern republican theory—freedom as non-domination" (Roberts 2015: 321). Desirable legislation might look something like the AI Act of the European Commission (see van Bekkum and Borgesius 2023; Veale and Borgesius 2021) or be responsive to the Biden White House's Blueprint for an AI Bill of Rights (Office of Science and Technology Policy 2022), even though each of these efforts may also fall short.

The neorepublican concept of domination is not only concerned with instances of technology interfering in peoples' lives in unjust ways. It is equally concerned with situations and infrastructural arrangements that make such interference *possible* and that create the potential for interference or that institutionalize domination within governments and the criminal justice systems. As Hoye and Monaghan (2018: 359) argue, one of the "foremost advantages" of neorepublican theory is "its capacity to address surveillance beyond the confines of non-interference, while also being able to address the best critiques of surveillance scholarship without jettisoning normative questions of freedom and unfreedom."

A neorepublican perspective highlights how critical surveillance scholars must consider the arrangements and broader infrastructures that create the space for the *possibility* of interference to occur and not to simply focus on and critique surveillance practices when they cause actual interference in peoples' lives. Encoding "semantic discontinuity" (Cohen 2012, 2013) or "gaps in enforcement and in systems of surveillance and control" (Balkin 2012: 81; see also Newell 2021) into the institutionalized and infrastructural surveillance arrangements present within our criminal justice systems should be informed by inclusive methods, such as, for example, the Diverse Voices framework developed by Young, Magassa, and Friedman (2019) that incorporates diverse input from affected communities. This involves amplifying the voices of stakeholders who may not typically be accounted for in technology policy and integrating their inputs into the policy formulation process. Incorporating human voices in the process of developing AI technologies and related policies (e.g., Friedman and Hendry 2019; Hartzog 2018) could minimize disparate impacts on marginalized groups by recognizing their values, needs, and concerns. This includes developing appropriate auditing for black box algorithmic systems (O'Neil 2016), but it also means more.

Importantly, there is room for creativity in devising new regulatory approaches to AI and similar technologies that consider the dominating potential of these tools. These regulatory efforts must bridge anti-discrimination, privacy, data protection, constitutional criminal procedures, and other areas of law related to protecting civil liberties by limiting algorithmic opacity and enhancing the transparency and accountability obligations of private companies and government agencies involved in deploying AI tools within the criminal justice system. Prioritizing those values aims to limit the potential for domination and injustice from opaque technological systems. Just as "the value of privacy…lies in its capacity to shield individuals from the threat of domination" (Roberts 2015: 321), other efforts to increase antipower and provide the ability of people to "command noninterference" (Pettit 1996: 589) and enjoy a "condition of resilient non-interference" (Pettit and Braithwaite 1993: 227) are equally necessary.

Acknowledgments

The authors express their gratitude to Andrew Roberts (Melbourne Law School) for offering insightful comments and feedback on this paper during its development, and to the anonymous reviewers who offered thoughtful and transformative feedback and suggestions. This paper is based on, and extended from, the first author's honors thesis (Huynh-Watkins 2021) and was written collaboratively by both authors.

References

Akbari, Azadeh. 2019. Follow the Thing: Data Contestations over Data from the Global South. *Antipode* 52 (2): 408–429.

Allen, Francis A. 1959. Criminal Justice, Legal Values and the Rehabilitative Ideal. *Journal of Criminal Law, Criminology and Police Science* 50 (3): 226–232.

Angwin, Julia, and Jeff Larson. 2016. Bias in Criminal Risk Scores is Mathematically Inevitable, Researchers Say. *ProPublica*, December 30. https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say [accessed December 12, 2023].

Balkin, Jack M. 2012. Room for Maneuver: Julie Cohen's Theory of Freedom in the Information State. *Jerusalem Review of Legal Studies* 6 (1): 79–95.

Barocas, Solon, and Andrew D. Selbst. 2016. Big Data's Disparate Impact. *California Law Review* 104 (3): 671–732.

Becker, Tim. 2020. City Council Approves Ordinances Banning Use of Face Recognition Technologies by City of Portland Bureaus and by Private Entities in Public Spaces. Portland.gov, September 9. https://www.portland.gov/smart-city-pdx/news/2020/9/9/city-council-approves-ordinances-banning-use-face-recognition [accessed April 26, 2023].

Bennett Moses, Lyria, and Janet Chan. 2018. Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability. *Policing and Society* 28 (7): 806–822.

Besson, Samantha, and José Luis Martí. 2009. Law and Republicanism: Mapping the Issues. In *Legal Republicanism: National and International Perspectives*, edited by Samantha Besson and José Luis Martí, 3–36. Oxford, UK: Oxford University Press.

Bigo, Didier. 2008. Globalized (in)Security: The Field and the Ban-opticon. In *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, edited by Didier Bigo and Anastassia Tsoukala, 5–49. Abingdon, UK: Routledge.

———. 2011. Security, Exception, Ban, and Surveillance. In *Theorizing Surveillance: The Panopticon and Beyond*, edited by David Lyon, 46–68. Abingdon, UK: Routledge.

Blunt, Gwilym David. 2015. On the Source, Site and Modes of Domination. *Journal of Political Power* 8 (1): 5–20.

Braithwaite, John, and Philip Pettit. 1990. *Not Just Deserts: A Republican Theory of Criminal Justice*. Oxford, UK: Oxford University Press.

Brayne, Sarah. 2021. *Predict and Surveil: Data, Discretion, and the Future of Policing.* Oxford, UK: Oxford University Press.

Brodkin, Jon. 2023. Black Man Wrongfully Jailed for a Week after Face Recognition Error, Report Says. Arstechnica, January 4. https://arstechnica.com/tech-policy/2023/01/facial-recognition-error-led-to-wrongful-arrest-of-black-man-report-says/ [accessed April 26, 2023].

Brown, Lindsay K., and Tiffany C. Veinot. 2021. Information Behavior and Social Control: Toward an Understanding of Conflictual Information Behavior in Families Managing Chronic Illness. *Journal of the Association for Information Science & Technology* 72 (1): 66–82.

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.

Brucato, Ben. 2014. Fabricating the Color Line in a White Democracy: From Slave Catchers to Petty Sovereigns. *Theoria: A Journal of Social and Political Theory* 61 (141): 30–54.

Capasso, Marianna. 2022. Manipulation as Digital Invasion: A Neo-Republican Approach. In *The Philosophy of Online Manipulation*, edited by Fleur Jongepier and Michael Klenk, 180–198. New York: Routledge.

Citron, Danielle Keats. 2008. Technological Due Process. *Washington University Law Review* 85 (6): 1249–1314.

Citron, Danielle Keats, and Frank Pasquale. 2014. The Scored Society: Due Process for Automated Predictions. *Washington Law Review* 89 (1): 1–34.

Cohen, Julie E. 2012. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven, CT: Yale University Press.

———. 2013. What Privacy is For. *Harvard Law Review* 126 (7): 1904–1933.

———. 2015. Studying Law Studying Surveillance. *Surveillance & Society* 13 (1): 91–101.

Conaboy, Richard, Henry Smith, and Richard Snyder. 1973. *The Criminal Justice Standards and Goals of the National Advisory Commission Digested from A National Strategy to Reduce Crime*. Pennsylvania Committee for Criminal Justice Standards and Goals. https://www.ncjrs.gov/pdffiles1/Digitization/54466NCJRS.pdf.

Crawford, Kate. 2021. *Atlas of AI. Power, Politics, and the Planetary Cost of Artificial Intelligence*. New Haven, CT: Yale University Press.

Dagger, Richard. 2009. Republicanism and Crime. In *Legal Republicanism: National and International Perspectives*, edited by Samantha Besson and José Luis Martí, 147–166. Oxford, UK: Oxford University Press.

Dencik, Lina, Arne Hintz, and Jonathan Cable. 2016. Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism. *Big Data & Society* 3 (2): 1–12.

Duarte, Marisa Elena. 2020. North American Indigenous Peoples Ruptured Knowledge Ecologies in Indian Country. In *Data Justice and COVID-19: Global Perspectives*, edited by Linnet Taylor, Gargi Sharma, Aaron Martin, and Shazade Jameson, 198–209. London: Meatspace Press.

Duke, Shaul, A. 2019. Database-Driven Empowering Surveillance: Definition and Assessment of Effectiveness. *Surveillance & Society* 17 (3/4): 499–516.

Ericson, Richard V., and Kevin D. Haggerty. 1997. *Policing the Risk Society*. Toronto, CA: University of Toronto Press.

Eubanks, Virginia. 2014. Want to Predict the Future of Surveillance? Ask Poor Communities. *The American Prospect*, January 15. https://prospect.org/power/want-predict-future-surveillance-ask-poor-communities./ [accessed May 1, 2023].

European Commission. 2018. EU Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, 237 final. Brussels, BE: European Commission. https://www.njb.nl/umbraco/uploads/2018/7/COM-2018-237-F1-EN-MAIN-PART-1.PDF [accessed December 12, 2023].

European Data Protection Board & European Data Protection Supervisor. 2021. Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence

(Artificial Intelligence Act) (pp. 1–22). https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf [accessed December 12, 2023].
Fan, Mary D. 2019. *Camera Power: Proof, Policing, and Audiovisual Big Data*. Cambridge, UK: Cambridge University Press.
Farid, Hany. 2018. The Dangers of Algorithmic Justice. TEDx, June. Video. https://www.ted.com/talks/hany_farid_the_dangers_of_algorithmic_justice [accessed November 7, 2024].
Ferguson, Andrew Guthrie. 2017. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.
Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. London: Penguin.
Friedman, Batya, and David G. Hendry. 2019. *Value Sensitive Design: Shaping Technology with Moral Imagination*. Cambridge, MA: The MIT Press.
Gandy, Oscar H. 1993. *The Panoptic Sort: A Political Economy of Personal Information.* Boulder, CO: Westview Press.
Gane, Nicholas. 2012. The Governmentalities of Neoliberalism: Panopticism, Post-Panopticism and Beyond. *The Sociological Review* 60 (4): 611–634.
Gargarella, Roberto. 2009. Tough on Punishment: Criminal Justice, Deliberation, and Legal Alienation. In *Legal Republicanism: National and International Perspectives*, edited by Samantha Besson and José Luis Martí, 167–184. Oxford, UK: Oxford University Press.
Gates, Kelly. 2019. Policing as Digital Platform. *Surveillance & Society* 17 (1/2): 63–68.
General, John, and Jon Sarlin. 2021. A False Facial Recognition Match Sent this Innocent Black Man to Jail. CNN, April 29. https://www.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html [accessed November 7, 2024].
Glenza, Jessica, and Nicky Woolf. 2015. Stingray Spying: FBI's Secret Deal with Police Hides Phone Dragnet from Courts. *The Guardian*, April 10. https://www.theguardian.com/us-news/2015/apr/10/stingray-spying-fbi-phone-dragnet-police [accessed November 7, 2024].
Gräf, Eike. 2017. When Automated Profiling Threatens Freedom: A Neo-Republican Perspective. *European Data Protection Law Review* 3 (4): 441–451.
Grinshteyn, Erin, and David Hemenway. 2016. Violent Death Rates: The US Compared with Other High-Income OECD Countries, 2010. *The American Journal of Medicine* 129 (3): 266–273.
Grossi, Giuseppe, and Daniela Pianezzi. 2017. Smart Cities: Utopia or Neoliberal Ideology? *Cities* 69 (September): 79–85.
Grother, Patrick, Mei Ngan, and Kayee Hanaoka. 2019. Face Recognition Vendor Test Part 3: Demographic Effects. NISTIR 8280. National Institute of Standards and Technology, December. https://doi.org/10.6028/NIST.IR.8280.
Guariglia, Matthew. 2022. Police Use of Artificial Intelligence: 2021 in Review. *Electronic Frontier Foundation (EFF)*, January 1. https://www.eff.org/deeplinks/2021/12/police-use-artificial-intelligence-2021-review [accessed December 12, 2023].
Hartzog, Woodrow. 2018. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge, MA: Harvard University Press.
Hayes, Ben. 2012. The Surveillance-Industrial Complex. In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty, and David Lyon, 167–175. London: Routledge.
Heydari, Farhang. 2022. The Private Role in Public Safety. *George Washington Law Review* 90 (3): 696–760.
Hill, Kashmir. 2020. Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match. *New York Times*, December 29. https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [accessed November 7, 2024].
Hillman, Noel L. 2019. The Use of Artificial Intelligence in Gauging the Risk of Recidivism. *The Judges' Journal* 58 (1): 36–39.
Hoffmann, Anna Lauren. 2019. Where Fairness Fails: Data, Algorithms, and the Limits of Antidiscrimination Discourse. *Information, Communication & Society* 22 (7): 900–915.
Hoye, J. Matthew, and Jeffrey Monaghan. 2015. Surveillance, Freedom and the Republic. *European Journal of Political Theory* 17 (3): 343–363.
Huynh-Watkins, Vincent. 2021. Abstracting Injustice: An Analysis of the Use of Artificial Intelligence in Criminal Justice. Undergraduate honors thesis. Eugene, OR: University of Oregon.
Joh, Elizabeth E. 2016. Beyond Surveillance: Data Control and Body Cameras. *Surveillance & Society* 14 (1): 133–137.
———. 2018. Artificial Intelligence and Policing: First Questions. *Seattle University Law Review* 41 (4): 1139–1144.
Johnson, Khari. 2022a. How Wrongful Arrests Based on AI Derailed 3 Men's Lives. *Wired*, March 7. https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/ [accessed December 12, 2023].
———. 2022b. The Hidden Role of Facial Recognition Tech in Many Arrests. *Wired*, March 7. https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests/ [accessed December 12, 2023].
Kaminski, Margot E., and Jennifer M. Urban. 2021. The Right to Contest AI. *Columbia Law Review* 121 (7): 1957–2048.
Lee, Adeline, and Laura Moraff. 2021. Surreal Stingray Secrecy: Uncovering the FBI's Surveillance Tech Secrecy Agreements. *ACLU*, December 15. https://www.aclu.org/news/privacy-technology/surreal-stingray-secrecy-uncovering-the-fbis-surveillance-tech-secrecy-agreements [accessed April 27, 2023].
Leslie, David. 2020. Understanding Bias in Facial Recognition Technologies: An Explainer. Preprint. Arxiv, October 5. https://arxiv.org/abs/2010.07023.
Leslie, David, Michael Katell, Mhairi Aitken, Jatinder Singh, Morgan Briggs, Rosamund Powell, Cami Rincón, Antonella Maia Perini, Smera Jayadeva, Anjali Mazumder, et al. 2022. Advancing Data Justice Research and Practice: An Integrated Literature Review. The Alan Turing Institute and The Global Partnership on AI, November. https://gpai.ai/projects/data-governance/advancing-data-justice-research-and-practice-an-integrated-literature-review.pdf [accessed April 26, 2023].

Levy, Karen. 2023. *Data Driven: Truckers, Technology, and the New Workplace Surveillance*. Princeton, NJ: Princeton University Press.

Linder, Thomas. 2019. Surveillance Capitalism and Platform Policing: The Surveillant Assemblage-as-a-Service. *Surveillance & Society* 17 (1/2): 76–82.

Lovett, Frank, and Philip Pettit. 2009. Neorepublicanism: A Normative and Institutional Research Program. *Annual Review of Political Science* 12: 11–29.

Lyon, David. 2003. Surveillance as Social Sorting: Computer Codes and Mobile Bodies. In *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, edited by David Lyon, 13–30. London: Routledge.

———. 2008. Biometrics, Identification and Surveillance. *Bioethics* 22 (9): 499–508.

Maas, Jonne. 2022. A Neo-Republican Critique of AI Ethics. *Journal of Responsible Technology* 9 (April): https://doi.org/10.1016/j.jrt.2021.100022.

Martí, José Luis. 2009. The Republican Democratization of Criminal Law and Justice. In *Legal Republicanism: National and International Perspectives*, edited by Samantha Besson and José Luis Martí, 123–146. Oxford, UK: Oxford University Press.

Masiero, Silvia. 2016. Digital Governance and the Reconstruction of the Indian Anti-Poverty System. *Oxford Development Studies* 45 (4): 393–408.

Metz, Rachel. 2020. Portland Passes Broadest Facial Recognition Ban in the US. CNN, September 9. https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html [accessed November 7, 2024].

Meyer, Joel. 1968. Reflections on Some Theories of Punishment. *The Journal of Criminal Law, Criminology, and Police Science* 59 (4): 595–599.

Monahan, Torin. 2018. Editorial: Algorithmic Fetishism. *Surveillance & Society* 16 (1): 1–5.

Morozov, Evgeny. 2013. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs.

Murakami Wood, David. 2013 What is Global Surveillance? Towards a Relational Political Economy of the Global Surveillant Assemblage. *Geoforum* 49 (October): 317–326.

Murakami Wood, David, and Kirstie Ball. 2013. Brandscapes of Control? Surveillance, Marketing and the Co-Construction of Subjectivity and Space in Neo-Liberal Capitalism. *Marketing Theory* 13 (1): 47–67.

Murakami Wood, David, and C. William R. Webster. 2009. Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example. *Journal of Contemporary European Research* 5 (2): 259–273.

Nakashima, Ellen. 2015. FBI Clarifies Rules on Secretive Cellphone-Tracking Devices. *The Washington Post*, May 14, https://www.washingtonpost.com/world/national-security/fbi-clarifies-rules-on-secretive-cellphone-tracking-devices/2015/05/14/655b4696-f914-11e4-a13c-193b1241d51a_story.html [accessed November 7, 2024].

Nellis, Ashley. 2016. The Color of Justice: Racial and Ethnic Disparity in State Prisons. The Sentencing Project, June 14. https://www.sentencingproject.org/publications/color-of-justice-racial-and-ethnic-disparity-in-state-prisons/ [accessed November 7, 2024].

Newell, Bryce Clayton. 2014a. Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information. *Maine Law Review* 66 (2): 397–435.

———. 2014b. Technopolicing, Surveillance, and Citizen Oversight: A Neorepublican Theory of Liberty and Information Control. *Government Information Quarterly* 31 (3): 421–431.

———. 2014c. The Massive Metadata Machine: Liberty, Power, and ~~Secret~~ Mass Surveillance in the U.S. and Europe. *I/S: A Journal of Law and Policy for the Information Society* 10 (2): 481–522.

———. 2018. Privacy as Antipower: In Pursuit of Non-Domination. *European Data Protection Law Review* 4 (1): 12–16.

———. *Police Visibility: Privacy, Surveillance, and the False Promise of Body-Worn Cameras*. Oakland, CA: University of California Press.

———. 2023. Surveillance as Information Practice. *Journal of the Association for Information Science & Technology* 74 (4): 444–460.

O'Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishing Group.

O'Neill, Natalie. 2020. Faulty Facial Recognition Led to His Arrest—Now He's Suing. Vice, September 4. https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing [accessed December 12, 2023].

Office of Science and Technology Policy [OSTP]. 2022. The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. The White House, October. https://www.whitehouse.gov/ostp/ai-bill-of-rights/ [accessed December 12, 2023].

Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

Perkowitz, Sidney. 2021. The Bias in the Machine: Facial Recognition Technology and Racial Disparities. *MIT Case Studies in Social and Ethical Responsibilities of Computing* (Winter): https://doi.org/10.21428/2c646de5.62272586.

Pettit, Philip. 1996. Freedom as Antipower. *Ethics* 106 (3): 576–604.

———. 1997. *Republicanism: A Theory of Freedom and Government*. Oxford, UK: Oxford University Press.

———. 2003. Agency-Freedom and Option-Freedom. *Journal of Theoretical Politics* 15 (4): 387–403.

———. 2008. Republican Liberty: Three Axioms, Four Theorems. In *Republicanism and Political Theory*, edited by Cécile Laborde and John Maynor, 102–130. Malden, MA: Blackwell Publishing Ltd.

———. 2012. *On the People's Terms: A Republican Theory and Model of Democracy*. Cambridge, UK: Cambridge University Press.
———. 2014. *Just Freedom: A Moral Compass for a Complex World*. New York: W.W. Norton & Co.
———. 2019. Neo-Liberalism and Neo-Republicanism. *Korea Observer* 50 (2): 191–206.
Pettit, Philip, and John Braithwaite. 1993. Not Just Deserts, Even in Sentencing. *Current Issues in Criminal Justice* 4 (3): 225–239.
Pugliese, Joseph. 2010. *Biometrics. Bodies, Technologies, Biopolitics*. New York: Routledge.
Ramiro, André, and Luã Cruz. 2023. The Grey-Zones of Public-Private Surveillance: Policy Tendencies of Facial Recognition for Public Security in Brazilian Cities. *Internet Policy Review* 12 (1): https://doi.org/10.14763/2023.1.1705.
Richards, Neil M. 2013. The Dangers of Surveillance. *Harvard Law Review* 126 (7): 1934–1965.
Rigano, Christopher. 2019. Using Artificial Intelligence to Address Criminal Justice Needs. *NIJ Journal* 2019 (280): 1–10.
Ritsema van Eck, Gerard Jan, and Lotte Houwing. 2020. A Republican and Collective Approach to the Privacy and Surveillance Issues of Bodycams: A Commentary. In *Police on Camera: Surveillance, Privacy, and Accountability*, edited by Bryce Clayton Newell, 223–230. Abingdon, UK: Routledge.
Roberts, Andrew. 2015a. A Republican Account of the Value of Privacy. *European Journal of Political Theory* 14 (3): 320–344.
———. 2015b. Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications. *Modern Law Review* 78 (3): 535–548.
———. 2018. Why Privacy and Domination? *European Data Protection Law Review* 4 (1): 5–11.
———. 2023. *Privacy in the Republic*. Abingdon, UK: Routledge.
Saulnier, Alana, and Diane Sivasubramaniam. 2021. Procedural Justice Concerns and Technologically Mediated Interactions with Legal Authorities. *Surveillance & Society* 19 (3): 317–337.
Schnably, Stephen J. 1991. Beyond Griswold: Foucauldian and Republican Approaches to Privacy. *Connecticut Law Review* 23 (4): 861–954
Selinger, Evan. 2022. "Reality+." Review of *Virtual Worlds and the Problems of Philosophy*, by David Chalmers. *The Philosophers' Magazine*, September 15. https://philosophersmag.com/reality-a-review/ [accessed November 7, 2024].
Selinger, Evan, and Woodrow Hartzog, 2020. The Inconsentability of Facial Surveillance. *Loyola Law Review* 66 (1): 33–54.
Simerman, John. 2023. JPSO Used Facial Recognition Technology to Arrest a Man. The Tech was Wrong. Nola.com, January 2. https://www.nola.com/news/crime_police/jpso-used-facial-recognition-to-arrest-a-man-it-was-wrong/article_0818361a-8886-11ed-8119-93b98ecccc8d.html [accessed May 3, 2023].
Skinner, Quentin. 2008. Freedom as the Absence of Arbitrary Power. In *Republicanism and Political Theory*, edited by Cécile Laborde and John Maynor, 83–101. Malden, MA: Blackwell Publishing Ltd.
Small, Deborah. 2001. The War on Drugs Is a War on Racial Justice. *Social Research* 68 (3): 896–903.
Smith, Patrick Taylor. 2020. A Neo-Republican Theory of Just State Surveillance. *Moral Philosophy and Politics* 7 (1): 49–71.
Srnicek, Nick. 2017. *Platform Capitalism*. Cambridge, UK: Polity.
Stafford, Mark, and Gini Deibert. 2007. Deterrence Theory. In *The Blackwell Encyclopedia of Sociology*, Volume 3, edited by George Ritzer, 1065–1067. Malden, MA: Blackwell Publishing.
Symons, John, and Ramón Alvarado. 2022. Epistemic Injustice and Data Science Technologies. *Synthese* 200 (2): https://doi.org/10.1007/s11229-022-03631-z.
Taylor, Linnet. 2017. What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally. *Big Data & Society* 4 (2): 1–14.
Taylor, Linnet, Gargi Sharma, Aaron Martin, and Shazade Jameson. 2020. What Does the COVID-19 Response Mean for Global Data Justice? In *Data Justice and COVID-19: Global Perspectives*, edited by Linnet Taylor, Gargi Sharma, Aaron Martin, and Shazade Jameson, 8–17. London: Meatspace Press.
Thompson, Heather Ann. 2019. The Racial History of Criminal Justice in America. *Du Bois Review: Social Science Research on Race* 16 (1): 221–41.
van Bekkum, Marvin, and Frederik Zuiderveen Borgesius. 2023. Using Sensitive Data to Prevent Discrimination by Artificial Intelligence: Does the GDPR Need a New Exception? *Computer Law & Security Review* 48 (April): https://doi.org/10.1016/j.clsr.2022.105770.
van Brakel, Rosamunde. 2021. How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium. *Surveillance & Society* 19 (2): 228–240.
van der Ploeg, Irma. 2005. *The Machine-Readable Body: Essays on Biometrics and the Informatization of the Body*. Maastricht, NL: Shaker Publications.
van der Sloot, Bart. 2018. A New Approach to the Right to Privacy, or How the European Court of Human Rights Embraced the Non-Domination Principle. *Computer Law & Security Review* 34 (3): 539–549.
van Sant, Shannon, and Richard Gonzales. 2019. San Francisco Approves Ban on Government's Use of Facial Recognition Technology. NPR, May 14. https://www.npr.org/2019/05/14/723193785/san-francisco-considers-ban-on-governments-use-of-facial-recognition-technology [accessed November 7, 2024].
Veale, Michael, and Frederik Zuiderveen Borgesius. 2021. Demystifying the Draft EU Artificial Intelligence Act—Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach. *Computer Law Review International* 22 (4): 97–111.
Villasenor, John, and Virginia Foggo. 2020. Artificial Intelligence, Due Process, and Criminal Sentencing. *Michigan State Law Review* 2020 (2): 295–354.
Voorwinden, Astrid. 2021. The Privatised City: Technology and Public-Private Partnerships in the Smart City. *Law, Innovation and Technology* 13 (2): 439–463.

Widra, Emily, and Tiana Herring. 2021. States of Incarceration: The Global Context 2021. Prison Policy Initiative, September. https://www.prisonpolicy.org/global/2021.html [accessed January 3, 2023].

Williams, Robert. 2020. Opinion: I Was Wrongfully Arrested Because of Facial Recognition. Why Are Police Allowed to Use It? *Washington Post*, June 24. https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/ [accessed November 7, 2024].

Wilson, Dean. 2019. Platform Policing and the Real-Time Cop. *Surveillance & Society* 17 (1/2): 69–75.

Wood, Stacy E. 2017. Police Body Cameras and Professional Responsibility: Public Records and Private Evidence. *Preservation, Digital Technology & Culture* 46 (1): 41–51.

———. 2019. Policing through Platform. *Computational Culture* 7: http://computationalculture.net/policing-through-platform/.

Young, Meg, Lassana Magassa, and Batya Friedman. 2019. Toward Inclusive Tech Policy Design: A Method for Underrepresented Voices to Strengthen Tech Policy Documents. *Ethics and Information Technology* 21 (2): 89–103.

Ziosi, Marta, Benjamin Hewitt, Prathm Juneja, Mariarosaria Taddeo, and Luciano Floridi. 2024. Smart Cities: Reviewing the Debate about their Ethical Implications. *AI & Society* 39 (3): 1185–1200.

Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30 (1): 75–89.

———. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.