Original Research Article

EJPT

European Journal of Political Theory
1–21

Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/14748851231203912
journals.sagepub.com/home/ept
Sage

Security, digital border technologies, and immigration admissions: Challenges of and to non-discrimination, liberty and equality

Natasha Saunders
University of St Andrews, UK

Abstract

Normative debates on migration control, while characterised by profound disagreement, do appear to agree that the state has at least a *prima facie* right to prevent the entry of security threats. While concern is sometimes raised that this 'security exception' can be abused, there has been little focus by normative theorists on concrete practices of security, and how we can determine what a 'principled' use of the security exception would be. I argue that even if states have a right to prevent migrants from entering on grounds of security, the practices required to implement this right will likely compromise core liberal democratic values in ways that have not been sufficiently appreciated. I draw on literature from Science and Technology Studies and Critical Security Studies to examine the proliferation of digital border control technologies which are increasingly dominating state security practices, and explain the challenges these technologies pose to non-discrimination, liberty and equality. I also highlight the difficulties of taking these principles as presumptive limitations on the operation of the security exception. A more sustained conversation among ethical theorists is needed to address the profound ethical challenges that the ever-increasing use of these technologies poses, particularly in pursuit of security.

Keywords

Borders, immigration, security, ethics, non-discrimination, liberty

Corresponding author:
Natasha Saunders, School of International Relations, University of St Andrews, Arts Faculty Building,
The Scores, St Andrews, KY16 9AX, UK.
Email: negs@st-andrews.ac.uk.

Introduction

Migration is increasingly spoken of, and acted upon, in public discourse and policy as a security issue, and migrants seen as threats to security.[1] So intertwined have migration and security become in the public consciousness and in political rhetoric, one might expect scholars working on the ethics of migration to have devoted considerable time and focus to discussing the intersection of migration and security. However, one would turn in vain to the scholarship of what is often referred to as the 'immigration admissions debate' for such an examination. What one is more likely to find is either silence on the issue of security as it relates to migration or, where it is mentioned, agreement that the state has a right to limit the entry of those considered to be security risks. While caution is sometimes expressed at the potential misuse of 'security' in migration (Carens, 2013: 175–176, 2003: 104, 1987: 260; Kukathas, 2021: 73–77) normative theorists of migration have yet to subject the issue to sustained examination. Rarely, if ever, is the question asked of what constitutes 'security'? What does it mean to be a security risk or threat? And how do we 'know' when someone is a security threat? While these questions have been extensively examined in Critical Security Studies, normative theorists should also be attentive to them, as the various possible answers have consequences for the type of action a liberal state *should* be allowed to take in the realm of migration control. As such, I do not make an argument for (or against) the right of a state to protect the security of its citizens – I take this as a given. It is one of the few points of (implicit) agreement between advocates of more open borders and advocates of the right of the state to exclude. Instead, I aim to shift normative attention to specific practices in migration control as they relate to security and reveal them as important sites of ethical reflection, through questioning what a principled approach to the security exception should entail. I argue that even if states have a right to prevent migrants from entering on grounds of security, the practices required to implement this right will likely compromise other core values in ways that have not been sufficiently appreciated.

The article is structured as follows. In the first section, I draw on the limited existing resources in the migration ethics literature on security to outline what, at a minimum, an ethical approach to the security exception could entail for a liberal democratic state. In the second section I introduce the reader who may be unfamiliar with them to developments in the realm of digitised border control practices and their intersection with the idea and practice of 'security'. The third section then examines some of the ethical challenges that the use of these technologies poses in light of the ethical approach to security I outlined in the first section. Through this discussion I draw attention not only to the challenges these technologies pose for the principles highlighted in the first section, but also to some important challenges in using these principles to limit the state's use of the security exception. A more sustained conversation among ethical theorists is needed, I conclude, to address the profound ethical challenges that the ever-increasing use of these technologies in pursuit of security poses.

Ethics and security

I argue in this article that while the basic premise of what I call the 'security exception' may be valid – that even if we argue for greater freedom of movement globally, the state may be justified in limiting the migration of people deemed security threats – many of the practices which states engage in to 'secure' the homeland from potentially 'dangerous' migrants are problematic from an ethical point of view. To demonstrate this, we first need to address two issues. First, what is 'security', and second, what might constitute an ethical approach to the security exception?

'Security' has traditionally been understood as the absence of threat, where that threat is understood to be existential in some way. This seems simple enough but raises more questions than it answers. How do we know when something or someone is an existential threat? And what is it threatening to? Physical survival (of what); a certain 'way of life' (of who); something considered particularly valuable (by who)? In other words, what is it that a government is supposed to 'secure'? The response of the US Government to the 9/11 attacks, and the criticisms of many of the policies implemented in their aftermath, are instructive here.

On 24 March 2004, former National Coordinator for Counterterrorism, Richard Clarke, opened his testimony before the September 11 Commission with the following statement: "Your government failed you. Those entrusted with protecting you, failed you; and I failed you. […] And for that failure I would ask for your understanding and for your forgiveness" (American Rhetoric, 2004). Clarke was speaking directly to the families of those killed that day, but also apologising to the wider public for failing to prevent an attack on something other than the lives of those killed. The attacks were perceived, fundamentally, as an attack on a particular *way of life* – one which takes freedom, equality and self-determination as its raison d'être. *America*, not only the individuals who died, was attacked that day. It seems, then, that what Richard Clarke thought the US Government had a responsibility to secure was not just the lives of individual citizens, but a particular way of life taken to be central to their understanding of themselves. Criticism of many of the actions taken by the US Government in the immediate aftermath of the attacks lends further weight to such an interpretation of security. Legislation, hastily passed with minimal debate in a climate of fear, such as the USA PATRIOT Act, facilitated one of the largest expansions of state surveillance of citizens in US history, and this surveillance disproportionately fell on Muslim-Americans and Arab-Americans. The PATRIOT Act has been criticised not only as undermining fundamental liberties such as the right to privacy and protection from unreasonable searches, but also as racially and religiously discriminatory – reducing some citizens to second-class status by virtue of their ethnicity and/or religion. The response to 9/11 can also be instructive for how the state treats non-citizens in relation to security, particularly relating to the green lighting of torture (under the pseudonym 'enhanced interrogation') and indefinite detention of 'enemy combatants' denied the usual protections of due process of law. These practices were also criticised as fundamentally undermining the very way of life it is claimed Al Qaeda attacked on 9/11. Such denials of fundamental rights are not only likely to backfire and make the state less secure, but are themselves actions unworthy of a liberal democracy supposedly committed to human rights (for further discussion, see Cole, 2003). On the face of it, then, it would seem that while ‘security’ for a liberal democracy certainly includes protecting the physical well-being of its citizens, such a state is limited in how it can act in pursuit of this security: in securing the well-being of its citizens, it must take care to avoid acting in such a way as to undermine the way of life those citizens find valuable.

As the above discussion indicates, identifying what ‘security’ means for a liberal democracy already takes us into the discussion of what an ethical approach to security should entail. While it would take an entire paper to develop a full ‘ethics of security’, we can turn to the limited existing engagements on the topic within the normative literature on migration to identify some candidates for principles that seem reasonable as baseline limitations on the practice of liberal states. The first is Carens’ insight that “the concept of national security can be and has been interpreted in such an expansive manner that it can be used to justify excluding anyone whom state authorities choose to keep out for any reason whatsoever” (2013: 175). To be morally permissible, Carens argues, the use of national security as a criterion of exclusion must be a ‘principled use’ (2013: 175). But what, exactly, does this mean? While he does not specify what would count as a principled use, his discussion does provide some examples of what seem to clearly be *unprincipled* uses: the increased scrutiny on Muslim migrants in the wake of 9/11; and the exclusion of LGBTQ migrants. It is, and has been, he argues, “all too easy to construct any category of immigrants as dangerous, thus smuggling back in under the national security banner forms of discriminatory exclusion that would be impermissible if used openly” (Carens, 2013: 175). We can take, then, as an initial principle that the security exception must not be used as a cover for morally arbitrary discrimination – that is, denial of entry, or increased surveillance/scrutiny, based on morally arbitrary characteristics such as race, ethnicity, gender, sexuality, and so on. I take this to be an unproblematic starting position as advocates of the state’s right to exclude and advocates of more open borders both agree (although for different reasons) that the state should not discriminate against potential entrants on such morally arbitrary grounds as these (e.g. Carens, 2003; Miller, 2005; Wellman, 2008).

Mendoza (2017) is the only normative theorist of migration that I am aware of who has attempted to tackle the issue of security head on, although he focuses on it in a different way to my treatment here. Mendoza focuses on the Plenary Power Doctrine, which grants to the US Federal Government complete discretionary control over immigration, shielding immigration decisions from judicial review. What this means in practice is that, when it comes to issues of admission, exclusion and enforcement, migrants attempting to settle and stay within the US lack core constitutional protections including the right to trial by jury, rights to court-appointed legal representation, and freedom from unreasonable searches and seizures. Security enters the picture here in two ways. First, it is supposedly for the sake of security that something like the Plenary Power Doctrine exists. In the Supreme Court decisions establishing the Doctrine, it is taken to be necessary to avoid the potential breakdown of order which an inability to control immigration would bring about. To protect stability and order, the government must have complete discretionary control to keep external threats at bay. Second, the exercise of the Plenary Power Doctrine itself gives rise to a security dilemma: it essentially abandons migrants to what Agamben calls a 'state of exception'. The dilemma here is the same as that identified above with the response to 9/11: that in prioritising security, the Plenary Power Doctrine creates another security problem. The security threat no longer menaces the state from the outside but has become an internal threat: the security of all – understood as a liberal democratic way of life under which individuals can pursue their life plans – is threatened by the unconstrained actions of the very government instituted to safeguard that security.

Mendoza argues that the way out of the security dilemma is to prioritise liberty concerns over security concerns – making respect for liberty a fundamental constraint on how the state can 'secure' itself. This means granting protections to immigrants that limit the discretionary powers of the state to control and enforce immigration policy. Border enforcement becomes unjust when it "uses certain intrusive methods or practices that infringe on the liberties of individuals in morally objectionable ways. A concern for individual liberty therefore places certain moral limits on the kinds of enforcement a legitimate state may properly implement" (Mendoza, 2017: 101). What counts as a morally objectionable infringement of individual liberty will vary with the context and the practice in question, which is one reason why it is so important that we examine actual practices, rather than remaining at the abstract level. But we can return to Mendoza's disquiet about the security dilemma to identify some individual liberties/rights that it might be reasonable to take as presumptive limitations on state practice in the name of security: rights to due process of law (such as a right to know what evidence is to be used against you, a right to a fair hearing and so on), equality before the law (we are all equally entitled to access due process and to be treated as such) and freedom from unreasonable searches and seizures (otherwise conceptualised as a right to a certain degree of privacy). We can combine this with Carens' non-discrimination requirement, such that we can say that, at a minimum, a liberal democratic state's policies in pursuit of security must avoid morally arbitrary discrimination, and must be presumptively limited in favour of basic individual liberties and universal equality before the law.

At this point we need to address a few important issues. Both Mendoza and Carens address the question of security with a focus on migration for the purposes of settlement, and enforcement of border controls on those already present. State security practice in the realm of migration certainly includes migration for the purposes of settlement, and internal enforcement, but goes further in an important respect. Individuals who may intend to travel to another state in order to inflict harm do not need to apply for the right to *settle* in order to do so. The 9/11 attacks, for example, were committed by individuals who had entered the United States on tourist visas, some of whom had overstayed without being flagged in time to the relevant federal agencies. Many of the security-related responses to 9/11 (both in the US and in many other states) thus target not only internal enforcement of immigration rules (such as visa overstaying), but also seek to prevent the *issuance* of tourist visas, limitations on visa waivers, and indeed deny access to global travel infrastructures, to people considered to be security risks.

As such, when it comes to the security exception, we must expand our focus beyond criteria for admission for the long term, and enforcement within the state, to how security practices extend ‘beyond’ the borders of the state to manage access to movement more broadly. The digital border technologies that I examine are intended to do precisely this. But this also raises two potential problems with the principles highlighted above for an ethics of security. Unlike Mendoza’s analysis of the security dilemma of the Plenary Power Doctrine, when it comes to preventing security threats from accessing the territory we are not dealing with problematic differential treatment of people *within* a liberal democracy. We are, instead, dealing with outsiders who wish to enter, or who simply wish to use global travel infrastructures. The second issue relates to the specific category of outsiders to which the security exception supposedly applies: those who are security risks. If the people the state is attempting to keep out, or render immobile, are threats to the security of the state, then why does the state owe any obligations to them at all?

There are two responses I would like to make to these issues, and they are connected. First, the fact we are dealing with outsiders does not permit a liberal state to violate the basic rights of non-citizens, or those outside the state, even if the action such a state should take in respect of those rights differs according to context. One is most likely to encounter a concern with security and migration in work advocating more open borders, and this work tends to ground arguments for greater freedom of movement in basic rights/liberties and concerns for universal equality. As such, these concerns should continue to matter in the expanded context of the use of the security exception. There are good reasons, however, for these principles – of non-discrimination, liberty and equality – to be of concern for advocates of the state’s right to exclude as well. As mentioned above, such arguments often stipulate that the right to exclude does not permit exclusion on the basis of morally arbitrary criteria such as race, gender and so on. Additionally, as I will show below, state control of migration for security purposes affects citizens and non-citizens alike. And so even if advocates of closed borders disagree that liberal democratic states have the same liberty and equality-based obligations to outsiders as they do to citizens, the security practices I highlight should still be of concern. The second response is that these issues show why attending to the specifics of *how security is practiced* is so important. ‘Security’ could, perhaps, provide a compelling reason to override the presumptive limitations that liberty and equality place on state policy. At the root of the second issue above – that we are dealing with people who are threats to the state – is an assumption that some people simply are threats to security and all we need to do is to identify them. But this is not how security practice actually works. As I will show in the proceeding sections, when it comes to practices that prevent the travel/entry of security threats, the kinds of technology used *constitute people as*, rather than *reveal them to be*, security threats. In summary, then, while the context in which the security exception operates differs from Mendoza’s security dilemma, which guide his argument in favour of liberty and equality as presumptive limitations on state practice, a focus on individual liberty and equality can still be valuable in helping us evaluate the use of the security exception by liberal democratic states. In what follows, I aim to explain not only the challenges that digital border control technologies pose to non-discrimination, individual liberty and equality, but also the challenges of trying to use these principles to control the use of the security exception in a rapidly digitising environment.

‘Securing’ borders from ‘risky travellers’

One of the legacies of 9/11 has been the increased securitisation of migration: a process whereby migration comes to be constituted in public discourse and practice as a security issue, and people on the move as potential security threats whose movement thus needs to be managed or prevented outright. Responses to 9/11 across a range of liberal democratic states contained a raft of measures designed to address this newly recognised ‘threat’, including a rapidly expanding digital architecture of migration management.[2] In a digital age, in which much of our lives are played out over the Internet, and for which we increasingly need smartphones and apps to carry out everyday activities, we constantly produce vast amounts of data about ourselves, our families, friends and acquaintances. Every time we connect to the Internet we generate vast digital traces (data) about our interactions, transactions, and movements (Ruppert et al., 2017: 1). Some of this data – such as the biographic or financial information that we put into a website – is personal data; other data – such as geolocation of photos we take on our smartphones – is metadata. While states have long gathered different forms of data about individuals, the explosion of the Internet age has given the state access to unprecedented volumes and forms of data. Personal data and metadata are considered treasure troves of useful information for states to make decisions about migration – whether that be an application for a long-term visa, for settlement, or for a tourist visa/visa waiver. States believe that the data we generate about ourselves can be used to determine how ‘risky’ it would be to allow us to board a plane or cross a border. Digital technologies such as machine learning, Big Data analytics, and the increased use of biometrics are being employed to make decisions on who can travel, where, when and how. The development and deployment of these technologies are justified as more efficient and effective ways to identify and keep out threats. The rest of this section will examine a few of these technologies/practices. The next section will then examine the ethical issues they raise.

Profiling

We tend to think that decisions about our ability to cross a border or to settle in a different state are made solely based on our own actions/biography, particularly where these align with the migration criteria of the state we are trying to enter. To a certain extent this intuition is correct. However, migration decisions are not based solely on what *we* have or have not *done*. They are also made based on beliefs about what someone ‘like us’ – from our state, of our age, with our travel pattern, engaged in certain ways on social media and so on – might (not) do in the future. In other words, states make use of profiling to decide who can cross borders, where and when. These profiles are increasingly built using data mining and analytics tools, which are put to work on aggregated data (massive volumes of (anonymised) personal and metadata of thousands of individuals).

Algorithms, perceived as able to ‘make sense’ of greater quantities of data than a person could, are used to identify ‘connections’ between data, people, events, organisations and so on, that indicate a ‘likelihood’ or ‘risk’ of engaging in criminal behaviour, terrorist activity and migration offenses such as visa overstaying. Border screening programmes, such as the current US Automated Targeting System, “subject passenger data to matching and profiling techniques to pre-check and score travellers for risk” (Hall, 2017: 488). Profiles are developed of potential behavioural and personal indicators – a model of what someone likely to commit terrorist activity, or overstay their visa, would act like and be like. Such systems, including those used during the visa approval process in many Western states, rely on large amounts of data, gathered not only from information we might provide to an airline when we book a ticket (Passenger Name Record data) – such as our name, payment method, passport information, meal preferences – but also information on friends, family and acquaintances that we might have to divulge during a visa application, or that can be mined from commercial databases and social media (Patel et al., 2019). Our data is run against the aggregated data of tens of thousands of others, to place would-be travellers into a specific category or a ‘risk pool’ to assist (or govern) decision making about travel (Adey, 2009). The whole logic behind profiling is not to identify *known* security threats – such as individuals already known to law enforcement or intelligence services – but to identify *potentially risky* subjects who are *not* yet known to the authorities. Being flagged during this profiling process could result in being denied a change in migration status, being placed on a No-Fly list, having a visa-waiver application denied, being required to attend a more in-depth interview at a consulate, being denied boarding at the airport, or being detained upon arrival.

Biometrics and ‘secure Id’

To protect the community from physical threats, states have a vested interest in being able to identify everyone seeking to cross their borders (whether on a short-term or long-term basis). This desire to be sure that ‘you are who you say you are’ is partly driving the global push for biometric identification systems. Biometrics refers to “the technology of measuring, analysing and processing the digital representations of unique biological data and behavioural traits” (Ajana, 2010: 238). These include fingerprints, iris scans, voice and facial patterns, and gait analysis. These technologies, some of them highly experimental, are increasingly being promoted as a silver bullet to combat ID theft and fraud, crime and terrorism, illegal work and so on, and to help states effectively govern access to things like immigration benefits (such as asylum support) (Ajana, 2010: 237). Biometrics can be used for identification/recognition, or for verification/authentication. Identification/recognition seeks to determine who someone is, by comparing their biometric (e.g. fingerprints) to the biometrics in the relevant database(s) – this is a one-to-many comparison. The Eurodac database, which contains the fingerprints of all asylum applicants in the EU and any apprehended irregularised migrants, follows this pattern. When a person lodges an asylum claim, their fingerprints are taken and run against the fingerprints in the database to identify whether they are a match for anyone already ‘in the system’. Verification/authentication seeks to determine whether a person is who they claim to be – a one-to-one comparison. Someone enrolled in a 'trusted traveller' programme and using an expedited border check process is an example of this. The person has already given their biometrics to the programme, and the scan – of their iris or their fingerprints – at the airport is compared to their previously enrolled biometrics to verify their identity and expedite their entry/travel.

Providing one's biometrics is increasingly becoming required for migration. Visa applicants must provide biometrics for entry to all Western states – usually a full set of fingerprints but this could also include an iris scan – at a consulate prior to attempting to travel. Refusing to provide one's fingerprints or iris scan will result in visa refusal. Powerful states are also able to use biometric requirements to influence the identity systems of other states. The US, for example, requires that any country that wishes its citizens to benefit from the US visa-waiver programme have, among other things, biometric passports ('e-passports'). Lacking a biometric passport means that you must go through the regular visa application process, even just to visit as a tourist.

Data sharing

To function, these digital practices, and others not examined in this article, require the data that we generate about ourselves. But when we use our smartphones or do things online, we often are not engaging directly with the state or deliberately providing our data to the state. For example, when I use Twitter, or check my credit score, I'm doing so for particular purposes and am engaging with specific companies. I'm not doing so to engage with my government, let alone any other government. So how does this data, often generated in a non-migration context, come to play a role in migration decisions? The short answer is data sharing.

Data sharing happens on several levels and between multiple actors: between the individual and the company running the app/website being used through agreeing to Terms and Conditions of use; between these companies and governments through contracts granting access to collected data; between agencies/government departments through shared access to databases; and between governments through data sharing agreements. A few examples should suffice here. To use Skype, one must agree to Microsoft's privacy policy. This privacy policy allows Microsoft to collect a wide range of data from users, but is ambiguous on the extent to which this data will be shared with others and what it will be used for. In some forced migration situations, such as the hotspots in Greece, asylum seekers were required to use Skype to engage with the asylum process, and thus were required to give Microsoft access to their data, and through them potentially other actors as well (Aradau, 2022: 39–40). These 'End User Licence Agreements' are rarely read and understood by most people. We click 'Yes' or 'Agree' because we must in order to use that app/service/website. But what we are agreeing to is to surrender ownership of the data that we produce as we use it. Once the company 'owns' that data, they can then sell it to others (Thatcher et al., 2016). For example, The US Immigration and Customs Enforcement agency (ICE) has purchased access to the Consolidated Lead Evaluation and Reporting (CLEAR) system from West Publishing Corporation and, in doing so, has gained access to a staggering array of data records including phone records, consumer and credit bureau data, healthcare provider content, utilities data, and data from social networks and chatrooms (Privacy International, 2020: 17). ICE uses this data to feed into its immigration enforcement activities. When an individual checks their credit score – perhaps with a view to applying for a credit card – they likely do not think that doing so will have any bearing on any plans they may have to migrate.

Sometimes, though, we do consciously and directly engage with the state and provide certain data in the process. We are often not aware, however, that this data can be and is also shared widely – between government departments, and even between states. When it comes to migration, this data sharing is often framed in the logic of security – for one state to adequately secure its homeland, it needs to share information to identify potential threats across various agencies responsible for security and migration, and it also needs information from other states. When applying for any kind of immigration status in the UK, applicants must sign a declaration stating that they understand that any information they provide to the Home Office may be shared with other government departments, agencies, the police, and even foreign governments. Further, that any data an applicant may have shared with these other actors, or which such actors may have acquired about the applicant, can be shared with the Home Office and used to make immigration decisions (Guild, 2019: 271).

What these kinds of declaration make clear is that data sharing is considered central to the ability of the state to make migration decisions, and that this is important for security. Indeed, the UK is part of the 'Five Eyes' intelligence community, with the US, Australia, New Zealand, and Canada. These states have agreed a data sharing protocol on travellers who arrive at one of their borders seeking immigration benefits (status or support) (Longo, 2018: 179). This kind of international data sharing is widespread, even if it may be most developed between the 'Five Eyes'. Multiple countries harvest data from commercial databases, and share them with agencies from other countries (Bellanova and de Goede, 2022: 107). In addition, cooperation agreements in the realm of migration between developed and developing states also involve the sharing of data on people on the move. A common condition of EU development aid, particularly through the EU Trust Fund for Africa, is the sharing of data with the EU, or with individual Member States, about people on the move. FRONTEX, the EU's border security agency engages, in social media monitoring for 'preventive risk analysis purposes', and shares information it generates with Member States (Latonero and Kift, 2018: 6–7). The proliferation and sharing of data is helping migration management become a "multisited system of remote control, in which detector tools capture and feed passenger data into networks that may be accessed by various state and non-state actors who are physically sited in multiple locations" (Broeders and Hampshire, 2013: 1209). Data, it seems, crosses borders far more easily than people.

Ethical implications

As shown above, the profiling of travellers to identify unknown security risks algorithmically generates perceived behavioural characteristics of real-life individuals based upon the aggregated data traces of thousands of others. The data that feeds into these profiles is only partly data that we consciously and deliberately make available to the state for migration purposes. The rest is data that we have no choice not to produce during our daily lives, but that governments can purchase and share with each other, and use to restrict the ability of people to move around. And more and more people, globally, are being required to prove their identity with their body in order to access global travel infrastructures. These are just some of the practices that states currently engage in to manage movement in pursuit of security. In what remains of this article, I draw on scholarship from Critical Security Studies and Science and Technology Studies to show how these technologies threaten commitments to non-discrimination, individual liberty and equality, but also the challenges of using non-discrimination, liberty and equality to try to control the use of the security exception in a rapidly digitising environment.

Non-discrimination

Public perception tends to view technology as neutral and objective – certainly more so than individual human beings are. Indeed, many of the technologies addressed above are marketed as such: digital technologies are not only posited as more effective and efficient at sorting and analysing information, but also are not hamstrung by the same prejudices as a human decision-maker. This is, however, a fundamental misapprehension. Technology is never neutral. Rather, it "reflects the values and interests of those who influence its design and use, and is fundamentally shaped by the same structures of inequality that operate in society" (Achiume, 2019: 4). In a series of Reports in 2019 and 2020, the United Nations Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Intolerance meticulously documented how the use of digital technologies such as algorithmic decision making, machine learning, Big Data analytics, biometrics and many others, can both directly and indirectly discriminate against people on a number of grounds, such as race, ethnicity, sexuality and gender, including in the context of migration and border control. These technologies reproduce biases that may be embedded in data sets (and thus reproduce implicit bias of humans), produce discriminatory results based on skewed data, gaps in data, and faulty assumptions underpinning the collection and classification of data. Data can also be intentionally manipulated – a particular concern when using data shared by authoritarian or repressive regimes (Achiume, 2019: 3). For example, states can use INTERPOL's Stolen and Lost Travel Documents system against political opponents, flagging their passport as stolen or fraudulent to prevent travel.

In most liberal states, it is already unlawful to use criteria such as ethnicity, religion, sexuality and so on, in a discriminatory way. The UK Home Office, for example, is not permitted to deny visas to people based on their ethnicity. In essence, this means that ethnicity (and other such criteria) is not permitted to be used as 'inputs' for decision making. However, even in the absence of a direct *intent* to discriminate (which using ethnicity or sexuality, for instance, as inputs for decision making would imply), *indirect* discrimination can result from using data/criteria that operate as proxies for race, ethnicity, gender, and sexuality – such as nationality, for example. A commitment to non-discrimination, then, must go further than focusing on data inputs, and also pay attention to the social, economic, political and historical contexts in which data are collected, digital technologies designed, produced, and put to work, and focus on tracking and addressing the *outcomes* of the use of these technologies over the long term (Mann and Matzner, 2019). This is a much more complex task than simply prohibiting the use of morally arbitrary criteria as data inputs for a digital process, as important as such a prohibition is.

Individual liberty

Recall above that profiling at the intersection of migration and security proceeds not only on the basis of what a potential migrant has done in the past but on the basis of perceived ‘behavioural potentialities’ (Adey, 2009: 277). There are a series of important, but fundamentally flawed, assumptions underpinning the use of algorithmic profiling. First, that there is a “self-evident relationship between data and people”, such that “we can interpret aggregated data to predict behaviour” (Metcalfe and Dencik, 2019); and, second, that the patterns algorithmically identified between data are reflective of such connections in the ‘real world’ – the algorithm merely overcomes limitations of the human mind to reveal connections that are ‘really’ there but that we just cannot see. As Leese explains, algorithmic profiling differs from more traditional, ‘confirmatory’ forms of profiling because the profiles are derived from the data being scrutinised (rather than being developed elsewhere and being used to confirm whether such characteristics are present in the data/population being scrutinised), and thus are inherently unstable and prone to fluctuation. The ‘profiles’ are not bounded by what is ‘known’ (about, say, past terrorists or visa overstayers), but consist of momentary groupings of characteristics derived from the ‘connections’ the algorithm makes between the data (Leese, 2014: 503). As things currently stand, issues with the quality and volume of data inputs mean that expertise from law enforcement and security professionals is often still needed to tweak targeting rules, and ‘clean’ faulty data (for more on this, see Glouftsios and Leese, 2023). We are not yet at the stage of completely automated profiling. However, what is vital to understand is that the connections that the algorithms make may not actually be connections in real life – they may only be ‘connections’ in the digital world of the algorithm (Longo, 2018: 159). Given enough data points, an algorithm can identify a ‘connection’ between them, but that does not mean this connection corresponds to anything in the non-digital world. ‘Our’ behavioural potentialities, then, are, in an important sense, not really even ours, and yet they can be assigned to us and used “to diminish a person’s range of future [migration] options” (Ajana, 2015: 69). As Ajana explains, the labelling of some people as risky and others as legitimate travellers “endows some with the right to smooth passage and reduced delay while others are made to endure an excess of bordering, sometimes before even leaving the country of origin” (2015: 66).

Understanding, at a basic level, how profiling works enables us to the see the problem with the assumption that these digital tools are a more effective and efficient way of identifying security threats whose movement must be managed. Rather than *revealing* security threats that were ‘already there’, but which we need an algorithm to see, these tools instead *constitute* people as security threats: you are a security threat because the algorithm says you are a security threat. If the data used to make such 'predictions' was only data we generate about ourselves then this would perhaps be less problematic. However, the data from which the profiles and their 'predictions' are derived are also aggregated data of unknown numbers of other people. What is at stake here is, in a fundamental sense, one's very status as an individual. When discussing individual liberty, it is easy to overlook the 'individual' half of the term. Within Critical Security Studies work which focuses on these digital technologies, the term 'Dividual' aptly describes what is at work here: the reduction of individuals to "bits and digits dispersed across a multitude of databases and networks" (Ajana, 2015: 72). It is these bits and digits that are 'recombined' by the algorithm and about 'whom' decisions are made, while the consequences of these decisions are felt by real-life individuals who may in reality bear little resemblance to the reconstituted 'person' about which the algorithm has made a decision. At root, then, what seems to be at stake here is the very status of the individual, and a right to be treated as an individual (even before one is treated as a citizen or non-citizen).

To come to the liberty half of 'individual liberty', a range of important basic liberties is threatened by the (digitised) security exception. Most obviously at stake with the use of biometric identification systems is freedom of movement – particularly the right to exit. It turns out that this right can be removed/curtailed not only by the repressive actions of an illiberal regime who actively bans emigration; it can also be violated by the global spread of biometric identification systems, often developed at the behest of, and with funding from, powerful liberal states in order to better secure their own societies. Recall that the purpose of a biometric identity system is to more accurately identify individuals, using something that we believe to be unique about each person: their fingerprint, or iris scan, for example. If we can rely on the body to reveal the truth about who a person is, then we do not have to rely on documents that might be fraudulent. On one level, this makes sense, certainly in relation to potential security threats. If we all must prove our identity with our body in order to travel then it becomes much more difficult for, say, someone on a terrorist watchlist to use fraudulent documents to board and hijack a plane. However, the right to leave one's own state and the right to seek asylum from persecution are both considered to be basic liberties of all, including non-citizens, that liberal democracies should respect. Biometric ID systems can pose significant threats to vulnerable/marginalised populations, precisely because they enable members of those populations to be more accurately identified. By making individuals more easily identifiable, they are made more vulnerable to abuse and repression. This has been flagged as a particular issue for the Rohingya populations in India, Bangladesh and Myanmar, all of whom are developing biometric ID systems with funding from Western states (Brinham et al., 2020). Facilitating this kind of identification becomes particularly serious in the event that a person feels they need to flee a persecutory situation. The ability to cross a border to safety may in fact depend on one's ability to *not* be identified, at least initially. Rohingya, for example, have often had to rely on the provision of fraudulent documents from intermediaries to board a plane and escape to a place of safety. This ability to move safely is being circumvented by the global spread of biometric ID systems, which require people to prove their identity with their body to travel.

This pushes people into the hands of smugglers and traffickers and exposes them to greater risk of violence and death.

Another important liberty put at risk by the current use of the security exception is freedom from unreasonable searches, which we could also cast in terms of the right to privacy. The discussion of data sharing and profiling earlier in this article highlighted that the data that feeds into these profiles is only partly data that we consciously and deliberately make available to the state for migration purposes. The rest is data that we have no choice to avoid producing during our daily lives, but that governments can purchase and share with each other to restrict the ability of people to move around. In our contemporary world it is almost impossible not to generate data about ourselves, and it is simultaneously almost impossible not to 'consent' to the potential sale or transfer of that data to other actors for uses that may not even occur to us. But at what point does this consent actually become an unreasonable search? The 'Terms and Conditions' to which we are obliged to consent to use services/apps/websites could certainly make it much clearer that our data – even if anonymised – can be sold and could be used for a range of purposes beyond that for which we originally provided it. But if there is no real option to opt-out of this data transfer and still use a service/app/website, then the choice we have is not between providing data about ourselves or not. It is, rather, a choice about using a service/app/website or not. This may not matter a great deal if what we are trying to use is relatively trivial, such as a restaurant booking app (although we have no way of knowing whether such activity or such an app would be considered trivial in a securitised migration context). But there are other services/apps/websites – such as Skype, for example – which we may be required to use for our job, or to connect with our families, or for which there is no comparatively data-lite option.

At stake here is what Longo calls the 'freedom to disappear into a realm of personal quiet' – a realm in which we are not 'internally invaded' by the collapsing of the boundary between us and the state (Longo, 2018: 165). Importantly, the collapsing boundary between us and the state is not just a boundary between us and our own state, but the boundaries between us and other states as well. Our data, even when anonymised, can still be used to build the profiles and targeting rules that work to prevent or hinder travel, and there is always a chance that we may run afoul of such profiles ourselves: "none of us stands outside these systems, even if individually we feel secure in our status as low-risk travellers, trusted borrowers or law-abiding citizens. We may feel insulated from coercive state power, but our data…all feed and train the algorithms that go on to make decisions concerning the treatment of other people" (Bradley and De Noronha, 2022: 63). There really is no way for us to determine which of our activities will be counted in a migration context, now or into the future, once such data are put to work for predictive analytics. A further challenge here is that even if it were feasible to *avoid* generating data about oneself, this 'clean skin' could itself be flagged as a risk marker (Allen and Vollmer, 2018: 24) that could also prevent our ability to travel or make the process significantly more expensive and time-consuming.

Equality/accountability

It appears, then, that digital border control technologies employed in pursuit of security threaten a range of basic liberties. What of equality concerns? On the one hand there may seem to be a fundamental equality at work in the operation of these border control technologies: everyone's data is potentially being captured and used. However, beneath this surface-level equality of treatment we can discern some threats to equality and challenges to taming the use of these technologies in pursuit of security, which come to the fore when we turn our attention to the ability to contest or challenge decisions to prevent travel for security reasons.

Privacy rights and data protection legislation are often posited as solutions to the data gathering and sharing problems raised by the increasing use of digital technologies in a variety of spheres of life. New legislation such as the EU's General Data Protection Regulation (GDPR), which governs access to personal data and give data 'subjects' the right to request what information is held about them, the right to have their personal data erased and so on, while generally extensive, is currently limited in important ways. First, GDPR protections are less accessible to migrants – and migrants may in fact be excluded from the protections/rights afforded to data subjects. The UK Home Office, for example, is able to use an 'Immigration Exemption' to its GDPR responsibilities where it would be likely to prejudice the 'maintenance of effective immigration control' or the 'investigation or detection of activities that would undermine the maintenance of effective immigration control' (Information Commissioner's Office, 2021: 323).[3] Should migrants be excluded from the protections given to data subjects in GDPR? While it is difficult to see a compelling reason why they should as a matter of course, things become more complicated when migration is considered to intersect with security. If all migrants were offered blanket access to the rights of data subjects then those potential migrants who may *want* to do a country or people harm would also be able to claim such rights/protections and could potentially enable them to work around security procedures and gain access to territory to inflict harm. To maintain the status quo, however, and retain a blanket exception seems too heavy-handed. Where should the line be drawn? How much information should a potential migrant be able to request?

Second, GDPR protections/rights only cover 'personal data' – data that could be used to identify a person. Metadata is often excluded, and yet, metadata also plays an important role in migration management in the name of security. If the metadata that we, and others, produce, and aggregated data – which often begins as personal data but is then anonymised – is also used to decide whether or not we can cross borders (and for what purposes) – by feeding into profiles, big data analytics and so on (Bellanova, 2017: 339) – then we should surely have a right to know what this data is and how it has been used. However, the very nature of metadata and the way it is used make this almost impossible. Even if we were informed about the broad nature of the metadata fed into an algorithmic system, we likely could not be informed about how the algorithmic system processed that data and produced the outcome it did. To understand why this is the case, and to understand the profound challenge this poses to the ability to challenge or contest decisions, we need to address accountability.

Accountability is important for equality, especially in terms of equality before the law and effective access to due process (whatever, depending on context, that process might be). Being able to challenge decisions we consider to be harmful, wrong, discriminatory and so on, or even simply to request that the rationale behind decisions be explained to us, is an important part of being recognised as equal before the law. Being in a situation in which no explanation is owed to you for, or being unable to challenge, a decision that materially affects your life, may be a sign that you live in a situation of domination.[4] But accountability is also a major challenge whenever an issue intersects with the realm of 'security', due to the existential stakes perceived to be involved. Information, sources of information, and how that information is used are kept secret so as not to reveal to one's 'enemies' what information one has about them. When migration intersects with security, secrecy also often follows. For example, individuals are not informed that their name has been placed on a 'No-Fly' list. You would only find this out when prevented from boarding a plane – and even then, you might have engaged a specialised lawyer to find out that you have been prevented from travelling because your name has appeared on a list. The US 'No-Fly' list is notorious for its scope (scope which pays no heed to citizenship) but also for the near impossibility of being removed from it if you do find out that you are on it and think that you should be removed (ACLU Southern California, 2013: 19). The US has never explained, and continues to refuse to explain, the criteria for inclusion on the list. This secrecy makes it almost impossible to challenge decisions to curtail one's ability to travel (not just to the state maintaining the list but to many/all states as this data is shared to prevent such individuals from taking more circuitous routes). Many of the digital practices highlighted above pose additional accountability challenges due to the nature of the technology being used.

Algorithms, such as those used in profiling practices, have been highlighted as opaque and unaccountable by nature. As Ananny and Crawford (2018) explain at length in their examination of transparency and algorithmic accountability, being able to see, understand, and govern complex systems in timely fashions is severely limited when it comes to algorithmic systems. Among the issues they highlight are the limits of understanding, technical limitations and temporal limitations. Even if we – or a group of independent experts – were able to 'see inside' an algorithmic system used in migration control, that does not mean that they (or we) would be able to *understand* the behaviour of that system and the rationale behind its decisions. Indeed, as Favaretto et al. (2019) highlight, "automatic decision-making might intrinsically transcend human comprehension since algorithms do not make use of theories or contexts as in regular human-based decision-making" (p. 17). This is especially the case for algorithmic systems that 'learn' – that adjust their decision making in light of new data inputs, rather than being tied to prior forms of reasoning based entirely on their training data. These sorts of algorithms do not, and cannot, give reasons for their decisions, nor, often, can their human programmers (Panagia, 2021: 116). If these obstacles could be overcome, then we would still face a temporal limitation to transparency/accountability. As Ananny and Crawford (2018) explain, even if an algorithm's source code, its full training data set, and its testing data were rendered visible, what we would see at that point is merely a 'snapshot of its functionality':

we would see the system at work at that particular point in time – not at a point in time earlier, or a point in time later than when we look inside (p. 982).

If accountability is, fundamentally, about the requirement of a decision-maker to 'account for' their decisions – to provide an explanation to an individual/group for the outcome of a decision-making process and/or for the decision-making process itself – then it is not immediately clear who or what we should expect to give an account of itself with algorithmic systems (Schuppli, 2014). An algorithm, of course, cannot give an account of itself. But it may perhaps also be problematic to expect the original designer or design team to do this – especially as many algorithms not only learn but are also part of a broader apparatus of control/decision making. We could require the relevant government department using the algorithmic system to be accountable for the decisions facilitated or made using them, but the ability to give such an account at least in part relies on the ability to understand how or why the algorithm has provided a specific output. Further, since we are concerned here with the intersection of migration and security, we cannot avoid the question of to whom accountability is owed, thus triggering, again, a concern with equality. Is it to all migrants, even those who may *want* to do the state harm? Recalling above that these technologies constitute people as security threats, rather than revealing them already to be such, how do we determine who is owed an account, and who is not, if these algorithmic systems themselves are supposed to tell us who is a threat and who is not, and it is this very decision for which we demand accountability?

The fundamental issue here is that if we do not, or cannot, know what data has been used to make a decision (or which bit of data proved decisive), who or what should be accountable for migration decisions made using these digital technologies? If the actor that we *decide* to hold accountable is unable to give a proper accounting of the rationale behind a decision, then this critically undermines individuals' ability to contest decisions that they believe to be wrong/discriminatory/harmful. Further, since the rationale of border externalisation is to make these decisions further and further away from the physical demarcations of territory, there are very real barriers to accessing any kind of redress for such decisions and harms (Shachar, 2020).

Conclusion

The technologies that I have outlined in this article may appear to be the incarnation of a perfect panoptic society, in which we are totally dominated by these digital technologies and the security logic they imbue. The state, it seems, is finally able to exert the kind of control over migration that it has longed for. Things are, of course, much messier than this. The kind of total control and taming of risk that the state may desire is frequently frustrated by technology failures, by incompatibility of databases, by legal challenges to contracts and the use of data, and so on (Glouftsios, 2021). Border agents do still exercise their own discretion when faced with information on their screens (Allen and Vollmer, 2018; Hall, 2017; La Fors-Owczynik and van der Ploeg, 2016). We do need to be wary, then, of positing total control. However, it is important to discuss this *now* precisely because this total control is not yet in place but is clearly the goal. Efforts are proceeding rapidly in this direction, and we usually only find out about them when organisations such as Privacy International force the hands of governments and make them reveal (some) information about exactly how ‘borders’ are controlled in the name of security.

The purpose of this article has been to show how complex the intersection of migration and security is, and to draw the attention of normative theorists of migration to the myriad practices that are involved in managing migration in an age where it is considered a security issue. States not only manage migration for the purposes of settlement, but seek to exert greater control over global movement more broadly, both to pre-empt attempts to settle but also to keep ‘security threats’ at bay. Their attempts to do so, I argue, may compromise core liberal democratic values of equality, liberty and non-discrimination. The management of movement and of security is becoming increasingly digitised, and as this evolving digital architecture grows, so too does the desire for data. What kind of data should the state be permitted to gather, purchase or share? How should the state be permitted to use the data it acquires? If the gathering and sharing of data is not territorially bound, should mechanisms of contestation or redress for migrants remain so? How can such mechanisms tame the panoptic tendencies of security-minded states? Commitments to non-discrimination, liberty and equality, given their supposed centrality to the identity of liberal democracies, should be central to answering these questions, lest we find ourselves in the kind of security dilemma that Mendoza warns us of. However, given the nature of the digital technologies being developed, using these principles to tame the operation of the security exception is not a simple task.

Acknowledgements

I am grateful to the participants of the Ethics of Border Controls in a Digital Age workshop (facilitated by the BISA Ethics and World Politics Working Group), to Anthony Lang, Jr, and to Alex Sager for their helpful comments and suggestions. My thanks also go to the anonymous reviewers and the editors at EJPT for their time and feedback.

Declaration of conflicting interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Natasha Saunders https://orcid.org/0000-0001-7651-0902

Notes

1. A note on my use of the terms migrant and migration: while most normative theorists focus on migration as migration for the purpose of settlement, I focus here both on migration for the purposes of settlement and migration more broadly – encompassing tourist travel, business travel, short-term migration and so on. Migration for the purposes of settlement is not the only form of migration that is managed/controlled by states, and other forms of movement – such as for tourism – are controlled *because* the state believes it necessary for security and to prevent potential settlement of undesirable individuals. For more on the value of thinking about migration beyond settlement in normative terms (see Altundal, 2022). In places where the term immigrant or immigration – to specifically refer to people entering with the intention of settling, I have used those terms.
2. For more general explorations of digital technology in border control and mobility management, and how these technologies are influencing/changing the meaning of security (see Amoore, 2006; Aradau and Blanke, 2018; Bellanova and de Goede, 2022; Bigo, 2014; Hall, 2017).
3. See the UK Home Office's Immigration Exemption Policy Document for examples of when the exemption may apply (UK Home Office Data and Identity Directorate, 2022: 6).
4. For recent work on domination and migration see Costa (2021), Honohan (2014) and Sager (2017).

References

Achiume ET (2019) Racial discrimination and emerging digital technologies: a human rights analysis. Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and racial intolerance (No. A/HRC/44/57). United Nations.

ACLU Southern California (2013) Muslims need not apply: How USCIS secretly mandates the discriminatory delay and denial of citizenship and immigration benefits to aspiring Americans.

Adey P (2009) Facing airport security: Affect, biopolitics, and the preemptive securitisation of the mobile body. *Environment and Planning D* 27: 274–295.

Ajana B (2010) Recombinant identities: Biometrics and narrative bioethics. *Bioethical Inquiry* 7: 237–258.

Ajana B (2015) Augmented borders: Big data and the ethics of immigration control. *Journal of Information, Communication & Ethics in Society* 13: 58–78.

Allen WL and Vollmer BA (2018) Clean skins: Making the e-Border security assemblage. *Environment and Planning D* 36: 23–39.

Altundal U (2022) The open borders debate, migration as settlement, and the right to travel. *Critical Review of International Social and Political Philosophy*: 1–25. https://www.tandfonline.com/doi/full/10.1080/13698230.2022.2040202

American Rhetoric (2004) Richard Clarke: Transcript of testimony before the 9/11 commission. https://www.americanrhetoric.com/speeches/richardclarke911commissiontestimony.htm (accessed 7.19.22).

Amoore L (2006) Biometric borders: Governing mobilities in the war on terror. *Political Geography* 25: 336–351.

Ananny M and Crawford K (2018) Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society* 20: 973–989.

Aradau C (2022) Experimentality, surplus data and the politics of debilitation in borderzones. *Geopolitics* 16: 26–46.

Aradau C and Blanke T (2018) Governing others: Anomaly and the algorithmic subject of security. *European Journal of International Security* 3: 1–21.

Bellanova R (2017) Digital, politics, and algorithms: Governing digital data through the lens of data protection. *European Journal of Social Theory* 20: 329–347.

Bellanova R and de Goede M (2022) The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance* 16: 102–118.

Bigo D (2014) The (in)securitization practices of the three universes of EU border control: Military/Navy – border guards/police – database analysts. *Security Dialogue* 45: 209–225.

Bradley GM and De Noronha L (2022) *Against Borders: The Case for Abolition*. London; New York: Verso.

Brinham N, Field J, Tiwari A, Ealom J, Arraiza J and de Chickera A (2020) Locked in and locked out: The impact of digital identity systems on rohingya populations. *The Institute on Statelessness and Inclusion*.

Broeders D and Hampshire J (2013) Dreaming of seamless borders: ICTs and the pre-emptive governance of mobility in Europe. *Journal of Ethnic and Migration Studies* 39: 1201–1218.

Carens JH (1987) Aliens and citizens: The case for open borders. *The Review of Politics* 49: 251–273.

Carens JH (2003) Who should get in? The ethics of immigration admissions. *Ethics & International Affairs* 17: 95–110.

Carens JH (2013) *The Ethics of Immigration*. New York: Oxford University Press.

Cole D (2003) Their liberties, our security democracy and double standards. *International Journal of Legal Information* 31: 290–311.

Costa MV (2021) Neo-republicanism and the domination of immigrants. *Res Publica (Liverpool, England)* 27: 447–465.

Favaretto M, De Clercq E and Elger BS (2019) Big data and discrimination: Perils, promises and solutions. A systematic review. *Journal of Big Data* 6: 1–27.

Glouftsios G (2021) Governing border security infrastructures: Maintaining large-scale information systems. *Security Dialogue* 52: 452–470.

Glouftsios G and Leese M (2023) Epistemic fusion: Passenger information units and the making of international security. *Review of International Studies* 49: 125–142.

Guild E (2019) Data rights: Claiming privacy rights through international institutions. In: Bigo D, Isin EF and Ruppert ES (eds) *Data Politics: Worlds, Subjects, Rights*. Abingdon: Routledge, 267–284.

Hall A (2017) Decisions at the data border: Discretion, discernment and security. *Security Dialogue* 48: 488–504.

Honohan I (2014) Domination and migration: An alternative approach to the legitimacy of migration controls. *Critical Review of International Social and Political Philosophy* 17: 31–48.

Information Commissioner's Office (2021) Gudie to the General Data Protection Regulation (GDPR).

Kukathas C (2021) *Immigration and Freedom*. Princeton, NJ: Princeton University Press.

La Fors-Owczynik K and van der Ploeg I (2016) Migrants at/as risk: Identity verification and risk assessment technologies in the Netherlands. In: van der Ploeg I and Pridmore J (eds) *Digitizing Identities: Doing Identity in a Networked World*. Abingdon: Routledge, 261–281.

Latonero M and Kift P (2018) On digital passages and borders: Refugees and the new infrastructure for movement and control. *Social Media + Society* 4: 1–11.

Leese M (2014) The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue* 45: 494–511.

Longo M (2018) *The Politics of Borders: Sovereignty, Security and the Citizen after 9/11*. Cambridge: Cambridge University Press.

Mann M and Matzner T (2019) Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society* 6: 1–11.

Mendoza JJ (2017) *The Moral and Political Philosophy of Immigration: Liberty, Security, and Equality*. Lanham: Lexington Books.

Metcalfe P and Dencik L (2019) The politics of big borders: Data (in)justice and the governance of refugees. *First Monday: Journal of the Internet* 24. https://firstmonday.org/ojs/index.php/fm/article/view/9934

Miller D (2005) Immigration: The case for limits. In: Cohen AI and Wellman CH (eds) *Contemporary Debates in Applied Ethics*. Malden, MA: Black, 193–206.

Panagia D (2021) On the possibilities of a political theory of algorithms. *Political Theory* 49: 109–133.

Patel F, Levinson-Waldman R, Den Uyl S, et al. (2019) Social media monitoring: How the department of homeland security uses digital data in the name of national security. *Brennan Center for Justice*.

Privacy International (2020) Submission to the "UN working group on the use of mercenaries" on the role of private companies in immigration and border management and the impact on the rights of migrants. *Privacy International*, London.

Ruppert E, Isin E and Bigo D (2017) Data politics. *Big Data & Society* 4: 1–7.

Sager A (2017) Immigration enforcement and domination: An indirect argument for much more open borders. *Political Research Quarterly* 70: 42–54.

Schuppli S (2014) Deadly algorithms: Can legal codes hold software accountable for code that kills? *Radical Philosophy* 187: 2–8.

Shachar A (2020) *The Shifting Border: Ayelet Shachar in Dialogue*. Manchester: Manchester University Press.

Thatcher J, O'Sullivan D and Mahmoudi D (2016) Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D* 34: 990–1006.

UK Home Office Data and Identity Directorate (2022) Immigration exemption policy document: Use of the immigration exemption under Article 23 of the UK GDPR and Schedule 2 of the DPA 2018.

Wellman CH (2008) Immigration and freedom of association. *Ethics* 119: 109–141.